SAND REPORT

SAND 2004-2696
Unlimited Release
Printed June 2004

Vulnerability of Critical Infrastructures: Identifying Critical Nodes

David G. Robinson
Roger G. Cox
September 2003

Risk and Reliability Analysis Department

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND 2004-2696
Printed June 2004

Vulnerability of Critical Infrastructures: Identifying Critical Nodes

David G. Robinson
Roger G. Cox

September 2003
Systems Risk and Reliability Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0748

drobin@sandia.gov
rgcox@sandia.gov

Abstract

The objective of this research was the development of tools and techniques for the identification of critical nodes within critical infrastructures. These are nodes that, if disrupted through natural events or terrorist action, would cause the most widespread, immediate damage.

This research focuses on one particular element of the national infrastructure: the bulk power system. Through the identification of critical elements and the quantification of the consequences of their failure, site-specific vulnerability analyses can be focused at those locations where additional security measures could be effectively implemented. In particular, with appropriate sizing and placement within the grid, distributed generation in the form of regional power parks may reduce or even prevent the impact of widespread network power outages. Even without additional security measures, increased awareness of sensitive power grid locations can provide a basis for more effective national, state and local emergency planning.

A number of methods for identifying critical nodes were investigated: small-world (or network theory), polyhedral dynamics, and an artificial intelligence-based search method – particle swarm optimization. PSO was found to be the only viable approach and was applied to a variety of industry accepted test networks to validate the ability of the apporach to identify sets of critical nodes. The approach was coded in a software package called Buzzard and integrated with a traditional power flow code. A number of industry accepted test networks were employed to validate the approach. The techniques (and software) are not unique to power grid network, but could be applied to a variety of complex, interacting infrastructures.

Contents

Figures ..... *vii*

Tables ..... *vii*

Movies ..... *vii*

Executive Summary *1*

1.0 Introduction *3*

2.0 Research Summary *5*

3.0 Power Grid Structure *7*

31. Government Agencies **7**

3.2 The Interconnections **8**

3.3 Grid Operation **8**

4.0 Bulk Power Reliability *10*

4.1 Background **10**

5.0 Contingency Analysis *14*

5.1 Background **14**

5.2 Challenges of Contingency Analysis **15**

5.2.1 Reducing the Contingency Set – Simplifying Assumptions 16

5.2.2 Reducing the Contingency Set - Implementation 17

5.3 Computational Issues **21**

5.4 System Performance Indices **23**

5.5 Other Contingency Analysis Issues **24**

5.6 Summary **24**

6.0 Node Identification *27*

6.1 Disruption of the System **27**

6.1.1 System Definition 27

6.1.2 Performance Measures 28

6.2 Complex Network Theory **28**

6.2.1 Background 28

6.2.2 Network Theory Basics 29

6.2.3 Approach 30

6.2.2 Conclusion 31

6.3 Polyhedral Dynamics **31**

6.3.1 Example 32

6.3.2 Simplicial relationships 33

6.3.3 q-Analysis Algorithm 34

6.3.4 Application 34

6.3.5 Polyhedral Dynamics Summary 35

6.4 Particle Swarms **36**

6.4.1 Background 37
6.4.2 Approach 38
6.4.3 Simple Example 40
6.4.4 Local versus Global Search 43
7.0 Implementation 48
7.1 Analysis Approach 48
7.2 Performance Measures 48
7.3 Power Flow Software 49
7.2.1 PFLOW 49
7.2.2 BPA/IPF 51
7.3 Buzzard 52
7.3.1 Buzzard Simulation Structure 53
8.0 Test Cases 55
9.0 Results 57
9.1 Enumeration: Exact Solution 57
9.2 Swarm Algorithm Implementation 60
10.0 Conclusions and Recommendations 64
10.1 Observations 64
10.2 Future efforts 64
Acknowledgements 65
Reference List 66

NOTE: A COMPANION CD OF MOVIE FILES IS AVAILBLE FROM DAVID ROBINSON (DROBIN@SANDIA.GOV)

Figures

Figure 1: NERC Regions 7
Figure 2: Eastern, Western Interconnections and ERCOT [1] 8
Figure 3: Types of Stochastic Reliability Analyses 11
Figure 4: Examples of Homogeneous and Scale-Free Networks 30
Figure 5: Simplicial Complex for Example 1 33
Figure 6: Critical Nodes for Complete IEEE 300 Bus Test System 35
Figure 7: Critical Nodes for IEEE 300 Bus Test System – System 1 Only 36
Figure 8: Sigmoid Function 39
Figure 9: Target Designations for Simple Example 40
Figure 10: Momentum versus Velocity – 5 agents:4 targets: 100 iterations 45
Figure 11: Momentum versus Velocity – 10 agents:4 targets: 100 iterations 46
Figure 12: Momentum versus Velocity – 5 agents:4 targets: 200 iterations 47
Figure 13: PFLOW Logic Diagram 49
Figure 14: PFLOW/Cassandra Analysis User Interface 50
Figure 15: Target System/Buzzard Interaction 52
Figure 16: Buzzard Swarm Interface 52
Figure 17: Buzzard Bulk Power Output Map 53
Figure 18: Buzzard/SCADA/Power Flow Information Exchange 54
Figure 19: Simple 5 Bus Test System 55
Figure 20: IEEE 300 Bus Reliability Test System 55
Figure 21: 69 Generator Reliability Test System 56
Figure 22: Distribution of Target Generators (2 Target Scenarios) 58
Figure 23: Distribution of Target Generators (3 Target Scenarios) 59
Figure 24 Final Velocities for Cell Size 7, Vmax=5.0, Momentum=[0.9-1.0] 62
Figure 25: Final Velocities for Cell Size 7, Vmax=[5.0-6.0], Momentum=1.0 63

Tables

Table 1. Relationships for Example 1 32
Table 2. Target Values for Simple Example 41
Table 3. Target Values for Momentum/Velocity Comparison 43
Table 4. Optimal 2 Target Sets : Truth 57
Table 5. Optimal 3 Target Sets: Truth 57
Table 6. Summary of Investigations for Target Size 2 or 3 60
Table 7. Summary of Investigations for Various Momentum, Vmax Values 61

Movies (files available separately)

Movie 1. Flock of Birds Foraging 38
Movie 2. Target Selection: $p_{g,t}, t = 5,10,\ldots,150$ 41
Movie 3. Grid Representation of Velocities 42

PAGE LEFT INTENTIONALLY BLANK

Vulnerability of Bulk Power Networks: Identifying Critical Nodes

David G. Robinson
Roger G. Cox

Risk and Reliability Analysis Department
Sandia National Laboratories

Executive Summary

The objective of this research was the development of tools and techniques for the identification of critical nodes within the national bulk power system. These are nodes that, if disrupted through natural events or terrorist action, would cause the most widespread, immediate damage. Until the tragic events of 11 September, 2001, experts in international terrorism felt that the ability to organize and execute a large scale coordinated attack was beyond the scope of terrorist organizations. Clearly we must change the way we view the vulnerability of our national assets. As the technology involved with the weapons being employed changes, so too must the people involved with their development and deployment. This research project was initiated in the summer of 2000 under the presumption that, contrary to conventional thinking at that time, this new breed of terrorist was evolving.

Through the identification of critical elements and the quantification of the consequences of their failure, site-specific vulnerability analyses can be focused at those locations where additional security measures could be effectively implemented. In particular, with appropriate sizing and placement within the grid, distributed generation in the form of regional power parks may reduce or even prevent the impact of widespread network power outages. Even without additional security measures, increased awareness of sensitive power grid locations can provide a basis for more effective national, state and local emergency planning.

Traditional contingency analyses performed by utilities are single point contingency analyses, focusing on identifying the single most critical element. In addition, analyses performed by utilities focus primarily on those elements which have a *naturally occurring* high failure rate, typically generation. Substations, transmission lines, etc. have low failure rates and so have low likelihood of inclusion in traditional investigations performed by utilities, but are exactly the easiest terrorist targets. The possibility of SCADA failures are also not considered in traditional analyses and are clearly vulnerable points of disruption through cyber attack on increasingly common operating system and network vulnerabilities. Finally, synergistic effects of multiple, simultaneous damage sites that can amplify the impact are not considered in traditional contingency analyses. In rough orders of magnitude, there are 10,000 potential points of attack in the western U.S. grid, 45,000 points in the north-east and 5,000 points in the Texas area. These are only the major generation and transmission elements and do not include command and control elements or elements that might be critical to a particular region.

In addition to the obvious costs to consumers and the direct impact on the U.S. economy, there are obvious national security implications associated with identifying and protecting these critical nodes. As noted in a special U.S. Senate report, the destruction of bulk energy systems would not only affect the ability of the U.S. to mobilize its forces, but would obviously impact the ability to support the war effort of a NATO member.

Through the identification of critical elements and the quantification of the consequences of their failure, site specific vulnerability analyses can be focused at those locations where additional security measures could be effectively implemented. In particular, with appropriate sizing and placement within the grid, distributed generation in the form of regional power parks may reduce or even prevent the impact of widespread network power outages. Even without additional security measures, increased awareness of sensitive nodes can provide a basis for more effective national, state, and local emergency planning. Locations and types of critical nodes can be used to preposition spares, deploy security forces, or be points where additional site security measures can be employed.

Identification of critical nodes or points of vulnerability within such a large, complex system is a daunting computational task. This research was focused on those situations where simultaneous, multiple points within the system would be attacked. To overcome the computational difficulties associated with traditional methods of vulnerability analysis, an artificial intelligence (AI) method was developed and applied to a variety of bulk power test cases constructed by the Institute of Electrical and Electronic Engineers (IEEE). The approach has a foundation in a branch of cultural psychology that can be used to model adaptive group behavior similar to that observed in flocks of birds and schools of fish.

The new method, an implementation of particle swarm analysis, successfully identified those critical combinations of network elements, which if disrupted, would possibly lead to a cascading series of events resulting in the most widespread damage.

The methodology is *technology independent*; it can be applied on not only bulk power systems, but also other energy systems or transportation systems. The methodology is scale neutral: it can be applied to power distribution networks at the local, state or regional level. However, complete validation and verification still must be accomplished before final implementation can be recommended. A cooperative effort with a large utility is the focus of future research efforts.

1.0 Introduction

Imagine for the moment that you are a terrorist. What particular elements of the national power grid (transmission lines, generators, substations, etc.) should you attack to cause the most damage? Developing the tools that can be used to answer that question is the goal of this project.

There are over 11,000 generation facilities, in excess of 200,000 miles of very high voltage transmission line and thousands of substations that constitute one of the largest machines ever constructed in the United States: the national power grid. Between 1980 and 1989 there were 5000 worldwide attacks against power transmission lines and towers; 386 of these were documented attacks against U.S. energy assets. The cost of a power disruption has been estimated to be approximately $1-$5 per kilowatt-hour including both direct and indirect costs. The outage in August 1996 covered an area from Canada to Mexico and from California as far east as Texas impacting over 7.5 million people and cost the state of California alone in the neighborhood of $1-$3 billion dollars. The outages in August 2003 impacted a considerable portion of the northeastern U.S. leaving approximately 50 million people without power in eight states and two Canadian provinces. Some preliminary estimates place the costs at over $6 billion dollars; the loss of revenue for just New York City has been estimated at half a billion dollars.

Deliberate attacks against power system assets occur for a variety of reasons and have a number of sources. The 386 documented attacks against U.S. energy assets between 1980 and 1989 include:

- Two Florida substations that were simultaneously dynamited in 1981, most probably as a result of a local labor dispute.
- Three 500-kV lines from the Palo Verde Nuclear Power Station that were simultaneously grounded over a 30 mile stretch in 1986. The plant was down for maintenance at the time so the reactors did not have to be shut down.

More recent events include the loss of power for four hours in five square mile of metropolitan San Francisco in October 1997 as a result of suspected substation sabotage. In October 2003, power distribution towers in Kalamath Falls (Oregon) were tampered with.

The actual number of attacks is understated since many attacks are not publicized due to the fear of encouraging further attacks. In addition to the obvious risks associated with physical disruption of the power grid, an additional vector for disruption of the power grid is through the control systems that manage the infrastructures. These control systems are referred to as Supervisory Control and Data Acquisition (SCADA) systems and operate via traditional and specialized communication architectures between grid substation and control centers.

The current state of world affairs clearly indicates that there is a high likelihood of additional, organized attacks.

This research effort concentrates on the identification of critical system elements, both the physical grid elements as well as the command and control structure. However, for

reasons of time and resources, a specific SCADA attack is not considered; however, the tools and techniques apply equally well to command and control elements as well as other types of infrastructures.

Through the identification of critical elements, site-specific vulnerability analyses can be focused at those locations where additional security measures could be effectively implemented. Even without additional security measures, increased awareness of sensitive nodes can provide a basis for more effective emergency planning such as the prepositioning of critical spares.

It is likely that, with possible differences in commercial and national security concerns, industry and government officials may not agree on the identification of critical power grid elements. An important aspect of this effort is the development of an analysis capability that can provide an objective assessment of the risks from a variety of different perspectives and that can be adapted to the unique needs of interested stakeholders.

2.0 Research Summary

Historically, utilities identify single points of vulnerability through a first-order contingency analysis. The list of candidate elements for disruption are identified *a priori* typically based on the rate at which the elements fail through the course of normal grid operation. Based on their naturally occurring failure rates, elements are randomly chosen from the list and removed from service. The reaction of the grid to the disruption is analyzed using a computer model of the power redistribution that results. Reliability indices are collected and the simulation of contingencies continue until convergence is reached.

The number of contingencies can explode rapidly: for a simple system of 69 potential points of failure, there are nearly $6x10^{12}$ different possible contingencies that could occur. For this reason the list of candidate elements is intentionally limited by analysts. For very large systems, the list is typically dominated by generation elements since transmission and substation failures are rare under normal bulk power system operation. The response of the bulk power system to these first-order contingencies is the basis for scheduling maintenance, setting reserve margins, emergency planning, etc. Unfortunately, as evidenced by the outages in 1996 and 2003, transmission lines can easily be home to an initiating event that cascades quickly.

Given the accessibility of transmission lines and substations to intentional disruption by terrorist organizations, it is important to develop a power systems contingency analysis approach that includes system elements beyond simply generation.

The objective of this research is to explore alternative, nontraditional methods of identifying critical elements in a bulk power system to improve contingency analysis. With the computational power available today, enumeration of all possible single point contingencies is a possibility. However, nonlinearities and synergistic effects preclude simply exploring and ordering all first-order contingencies.

The focus of this research is the development of a methodology that can be used to identify the second-, third-, and higher order contingencies. Contingency analysis has been the focus of much research the past few years but the emphasis has remained on naturally occurring failures rates. It was decided that, rather than duplicating the direction of these research efforts, a more theoretical systems approach would be emphasized.

A trio of very different approaches is investigated. The first involves complexity theory and network theory in particular. Network theory has been applied extensively on a wider variety of complex networks including communication networks, the Internet, and even power systems. The goal of these efforts has been to characterize the robustness, fragility, and attack tolerance of complex networks. Large networks can be typically classified into two groups: homogeneous and non-homogeneous. Nodes in homogeneous networks typically have roughly the same number of connections. Random graphs and small-world networks are examples of homogeneous networks. Nonhomogeneous, or scale-free networks are largely homogeneous, but contain a few nodes that are highly connected. The Internet and World Wide Web are examples of scale-free networks.

Scale-free networks typically result from an evolving system with preferential points of interconnection. The robustness (or inversely, the fragility) of large networks is characterized by their diameter, the average length of the shortest path between two nodes. The fragility of a network is investigated as highly connected elements are removed and the diameter of the network changes.

A second approach investigated in this research involves characterizing the bulk power system as a complex series of *n*-dimensional polyhedra, similar in many ways to a large crystal. The vulnerable points on the grid expose themselves as 'cleavage' points in the crystalline structure. Polyhedral dynamics, a branch of set theory that deals with the topological relationships between finite sets, is employed to relate the various elements of the power network to a simplicial structure and to identify the vulnerable points in the network.

The final and most promising research focused on the use of an AI-based approach founded in cultural psychology. The swarming behavior of flocks of birds and schools of fish are used as a basis for finding the optimum combination of network nodes to be disrupted to cause the most damage.

This report begins by discussing background in the physical and regulatory structure of the bulk power system. A review of existing bulk power reliability and contingency analysis methods is then provided. This is followed by a more detailed discussion of the three approaches investigated to identify critical nodes (and mentioned briefly above). Implementation of the most promising method is then discussed and the results from a number of test cases are provided. Finally, conclusions of the research and recommendations for future efforts are presented.

3.0 Power Grid Structure

31. Government Agencies

The North American power grid is composed of four major synchronous interconnections that are further divided into ten regional reliability councils. Each reliability council has primary responsibility for maintaining electric system reliability in its region, involving coordinating the activities of numerous control centers belonging to individual utilities, power pools, or independent system operators. Together, the reliability councils compose the North American Electric Reliability Council (NERC), which sets overall reliability policies and standards.

For example, the Western Electricity Coordinating Council (WECC) is one of 10 electric reliability councils in the US (Figure 1). The WECC provides a forum for coordinating the operation and planning activities of its 104 member systems to assure electric system reliability for an area covering approximately one-half of the US. These members represent the broad spectrum of interests in the electric industry and 76 electric utilities including PG&E, Sacramento Municipal Utility District, the Santa Clara and Palo Alto municipals, Southern California Edison, and San Diego Gas and Electric. The grid serves over 59 million people in 14 western states, two Canadian provinces, and one Mexican state

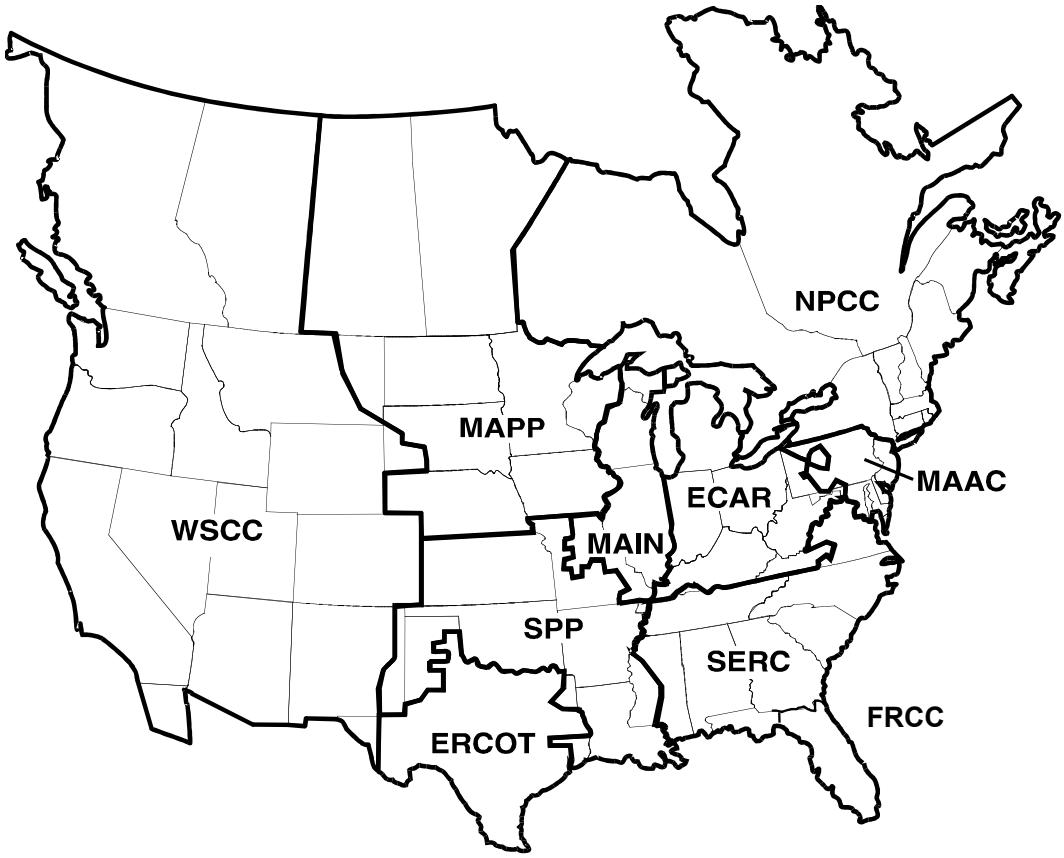


Figure 1: NERC Regions

The Federal Energy Regulatory Commission (FERC) is an independent government regulatory agency that oversees the interstate transmission and sale of oil, natural gas and electricity. The commission consists of five members serving 5-year presidential appointments and is funded via a 'tax' on commercial agencies that fall under the FERC regulatory umbrella.

3.2 The Interconnections

The electrical system in North America consists of three major predominately U.S interconnections and the loosely tied Quebec interconnect (Figure 2). The generation and demands within each interconnection are physically connected and operate almost autonomously. The largest of these interconnects is the Eastern Interconnect covering the eastern two-thirds of the U.S. and Canada across the area from Nova Scotia, Canada to Florida and from Saskatchewan, Canada to eastern New Mexico. The Western Interconnect is the second largest and has several direct current connections with the Eastern Interconnect. The Western Interconnect covers approximately eleven western states, southwestern Canada and northwestern Mexico. The smallest interconnect, ERCOT (Electric Reliability Council of Texas), services approximately 85% of the Texas electrical demand. While the ERCOT Interconnect is tied with Mexico, it is not tightly connected with either the Eastern nor Western interconnects.

3.3 Grid Operation

While the grid as it exists today is physically different from the grid of yesterday, there are major differences in how the grid is operated today when compared to thirty or forty years ago.

In the past, power was utilized in close geographic proximity to its generation site; there were few transfers of power between utilities. In the event of an emergency, utilities relied on neighboring utilities for reserve power generation. In contrast, today there are thousands of power transfers every day and power flows cover thousands of miles. The

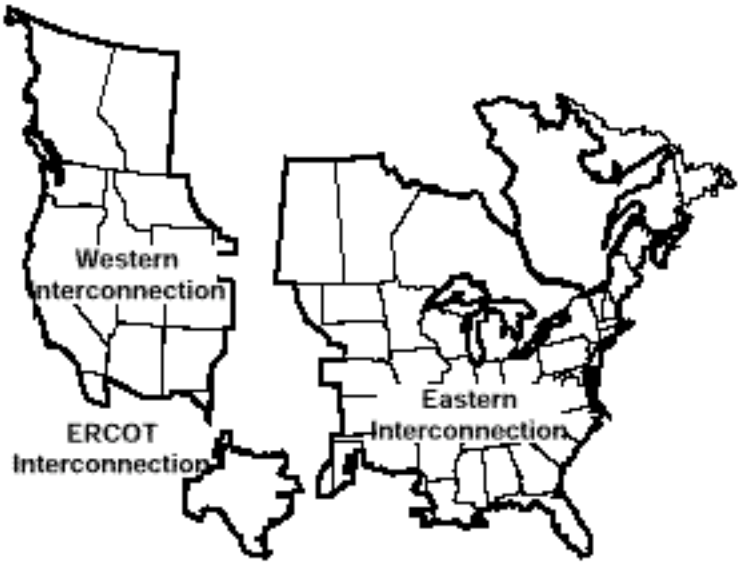


Figure 2: Eastern, Western Interconnections and ERCOT [1]

grid is now being used as a national level resource with significant geographic, social and network barriers between ‘neighbors’. This change to an open system at a national level has been encouraged by FERC since about 1996 under the supposition that such an approach will lead to substantial savings in energy costs for the consumer. Unfortunately this has lead to the grid being operated in a manner inconsistent with the current physical structure of the grid. The increase in power flow transactions has resulted in the situation where generation and transmission outages in a few areas have a strong impact over thousands of miles. It remains to be seen if the anticipated savings to consumers will exceed the cost of the future blackouts.

4.0 Bulk Power Reliability

4.1 Background

Electric power systems are intended to supply customer load with voltages within a specific range, without overloading components such as transmission lines. A power system failure (commonly known as a 'blackout' or 'brownout') occurs when, in response to disturbances such as transmission line outages, a transition cannot be made from one *acceptable* steady state to another.

In a normal or acceptable state, power balance is guaranteed at all points in the system. Power is generated primarily by rotating machines and consumed to a large extent by rotating loads. Power balance implies that these machines operate at essentially constant speed as evidenced by an essentially constant frequency. Similarly, loads that regulate their energy consumption (e.g., thermostatic loads) achieve a steady pattern of operation. Any departure from power or energy balance initiates a dynamic response from the generators, loads and other regulated equipment, in an effort to establish a new steady state. A new steady state may be established with power balance but unacceptable conditions. On the other hand, the dynamics of the system may be such that the system cannot transition to a new steady state even if one exists. This is referred to as *instability*.

A failure sequence may take several forms including:

- A disturbance drives the system into a state wherein a steady state power balance exists, but voltages or loadings are out of limit. Further, the condition cannot be corrected due to time constraints or lack of resources. In this instance, typically, some load is disconnected. This is often called 'loss of load' or 'load shedding'.
- A disturbance creates a condition in which changes in power or voltage are so severe that protective mechanisms initiate the dropping of load and perhaps separation of the system into islands.
- A disturbance creates a condition where a steady state power balance cannot be achieved at all.
- A disturbance creates a condition in which system dynamics/control is unstable. For analytical purposes such instability is classified as follows:
    - *transient or angle instability*: the electromechanical dynamics are such that the generators cannot be returned to a common operating speed. The time range of this phenomenon is 1-3 seconds.
    - *long term instability*: the control systems are underdamped or undamped, resulting in oscillatory behavior over a long period of time (minutes) and operation of protective systems.
    - *voltage instability*: involves system response in terms of regulating system voltage and is a function of the ability of the generators to maintain voltage(provide reactive power), the response of loads such as motors to low voltage conditions, and the response of thermostatic loads which attempt to continue to draw the required energy by cycling more

frequently, for example. The result may be a very rapid uncontrolled decline in voltage (voltage collapse) or a very slow decay (period of hours)

In the event of a failure the above phenomena occur simultaneously, but depending on the system state, one form may be dominant.

The general definition of *acceptability* is that disturbances should not result in loss of load. Indeed, reliability councils have adopted a deterministic concept of operational reliability as one in which anticipated disturbances do not cause an 'uncontrolled loss of load'. The terms 'adequacy' and 'security' have been standardized in power industry literature to describe power system reliability and are depicted in Figure 3 [2,3,4].

- *adequacy* refers to the ability of a system to supply load in the steady state. Dynamics of transition are ignored
- *security* refers to a the ability to return to a steady state (i.e. presumes stability of state transitions).

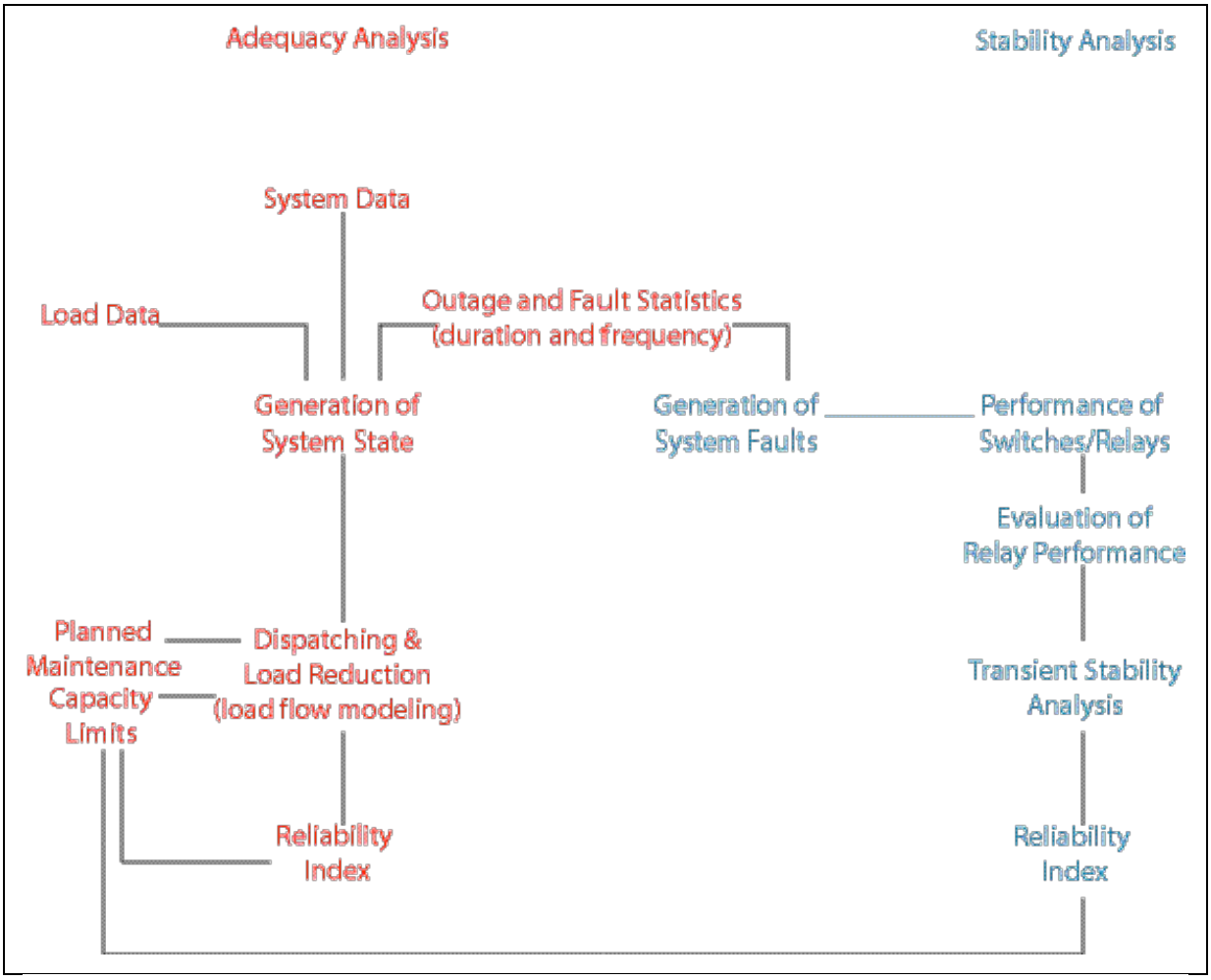


Figure 3: Types of Stochastic Reliability Analyses

(There is less than complete consensus on these definitions. The definitions have been paraphrased based on what appears in literature. A more common use of the term 'security' is in an operational context with reference to a specific state.)

The reason for this distinction is that the study of system dynamics is extremely computationally intensive. Further, the random events that initiate a change of state involve fundamental phenomena such as lightning induced short-circuits, which are not easily modeled in security analysis. Adequacy analysis on the other hand involves more manageable models. A bulk power system is typically modeled by static, nonlinear models, while random events are more macroscopic, such as the outage of a transmission line. *Adequacy analysis provides an upper bound on reliability measures*.

Given the computational burden of reliability analysis, approximate models are often used even for adequacy analysis. In terms of the conceptual modeling, the following approximations are often used:

- Generation adequacy studies which ignore the transmission system.
- Transportation model based bulk-system studies ignore ohms law and merely look at power transfer along capacitated arcs (transmission lines).
- *dc* load flow studies which are a linear approximations to circuit equations and model the nature of real power (watts) flow through the network.
- Static power flow studies, or ac power flow studies, which calculate the *operating voltages, line power flow,* etc., for a given condition and determine whether these quantities are acceptable.
- Extended static power flow studies, which include sensitivity analysis, optimization, and operating margin studies.
- Short term dynamics studies such as transient stability studies, which determine if a proposed disturbance leads to instability. Both time-domain simulations and direct methods are used.
- Long term dynamic studies such as mid- and long term stability and voltage collapse.

Most reliability studies focus on generation systems, and bulk system adequacy studies using *dc* or *ac* power flow models. As such they are not used to direct system planning, but as checks on candidate plans. Alternatively, power system expansion planning involves exhaustive studies of a limited number of scenarios with detailed dynamic analyses.

The degree to which a bulk power system operates in an acceptable manner is described by various indices. An example of a deterministic index is the commonly used criterion that there should be no load shedding upon loss of a single major component (the [n-1] rule, heavily used until roughly 1995, but still commonly used in planning today). An example of a probabilistic index is the Loss of Load Probability or Loss of Load Expectation.

A comprehensive calculation of probabilistic indices is considered to be computationally intensive. Barriers to such computation include:

- Problem dimensionality; power systems are extensively interconnected and may contain 20,000 or more components relevant to system reliability; the state space may not be coherent.
- Discrete nature of failure distributions.
- Successful operation involves both acceptable steady state operation in terms of voltage levels and power flow conditions, as well as stability with respect to dynamic conditions. A load shedding event can occur due to unacceptable voltages or loading in the steady state after an event, the non-existence of steady state equlibria, instability of equlibria or transitions, and operating policies such as protection schemes. Thus, comprehensive evaluation of even a single state is a difficult problem.
- Complex failure modes of components; examples are partial failures in generating plant (derated conditions), common-mode failure of system components, etc.
- Temporal dependencies; parameters such as load, the generation from energy dependent resources, etc., represent stochastic processes.

Traditionally, because of the computational burden, deterministic criteria have been used to develop planning decisions, while probabilistic criteria have been used for comparative analysis and reporting purposes. Some observations from a review of the literature:

- Bulk power reliability has been and continues to be the subject of research in the power systems area. Current trends toward deregulation have shifted research towards the related areas of probabilistic production costing, deterministic security analysis, and risk analysis.
- Typically, reliability studies in published literature only address adequacy -- i.e., steady-state operation of the network.
- Analytical studies have been limited to generation system adequacy analysis, which is essentially a linear problem. In these studies, the network is ignored.
- Bulk or composite system reliability analyses utilize contingency analysis, Monte-Carlo simulations, or a combination. The contingency analysis essentially involves enumeration of selected states followed by an analysis of the steady-state model. Monte-Carlo sampling methods involve sampling states from prescribed distributions and analysis based on the steady-state model.

In this study, due to the extensive number of system states to be investigated, only the steady-state operation of the network (power adequacy) is considered and only deterministic criteria are used. Even without the excuse of computational burden, it is common for preliminary analyses of bulk power systems to have these boundaries. It is expected that upon identification of critical system states, a more thorough investigation of system reliability will be conducted.

5.0 Contingency Analysis

5.1 Background

A commonly used approach to reliability assessment of the power grid involves identifying a series of contingencies or events, exercising a power flow model based on these events, and then observing the adequacy of the network. Given the adequacy, corrective action is taken: rescheduling of generation, tripping overloaded transmission lines, load shedding, etc. Network adequacy is again checked and performance indices are calculated. This stochastic analysis is often too computationally intensive and an alternative approach is used: contingency analysis.

Contingencies are constructed by randomly selecting a set of failed grid elements. For computational reasons, these contingency sets are typically restricted to the failure of a single grid element; this is typically a generation unit, since transmission lines are assumed to have a very, very low likelihood of failure. The response of the bulk power system to these first-order contingencies is the basis for scheduling maintenance, setting reserve margins, emergency planning, etc.

The non-linear behavior of power networks and rapid propagation of failure events make formal contingency analysis critically important. These same non-linearities, coupled with the size of the network and the uncertain nature of demands and environmental conditions, make modeling to support contingency analysis particularly difficult.

Formal contingency analysis has been an active R&D focus since the 1960s, and a number of survey papers have been written on the topic of power grid modeling and contingency analysis [5-9]. Contingency analysis is basically a perturbation analysis on existing power flow analytic and simulation models. These existing computer models assess the adequacy of a specific power grid configuration (generation and transmission) to meet a forecast load set. Normally, there is some policy in place at the utility or control region level to ensure no contingencies of a particular type or likelihood will compromise the system to some level. The technical objective is to identify all those contingencies that result in system failure or compromise at some level, and ensure none of the relevant contingencies is in this set. There has been discussion of extending this to formally look at the mean time between failures (MTBF) and mean time to repair (MTTR) of contingencies in order to incorporate measures of system availability into policy analysis [10].

The perturbations of contingency analysis are alternative power grid configurations based upon potential system failure events. Failure events involve major elements of the power network: generators, transmission lines, buses, circuit breakers and transformers. Such failures can be total or partial. Failures are generally assumed to be independent, although common mode failures such as weather-related failures and line outages are also identified and processed. Outage rates of transmission lines are assumed to be weather-related, whereas other equipment is assumed independent of the weather. Circuit breakers can fail during normal conditions (like a bus) or fail when called upon to perform, such as failing to open. Other such contingencies that are known *a priori* to be

important can be manually added to the contingency set; these are known as must-run contingencies.

The resulting performance level, or system adequacy, of the power grid to a failure event is captured in numbers known as **indices**. Indices reduce the multidimensional nature of power system performance to a single number. In contingency analysis, these indices are used for ranking and screening of various scenarios. There are two types of indices: system problem indices that ignore remediation, and severity indices that reflect remediation actions. Performance indices can be the output of a model, or estimated after the fact from power flow model calculations.

The difficulty with this approach is that one must already have effectively identified what the critical grid elements are before performing a traditional critical node analysis. As evidenced by the single point failures of the western power grid that left 2 million people without power in July 1996, and 5.6 million people without power in August 1996, the traditional approach of using first order (i.e. [n-1]) contingency analyses does not necessarily identify system elements that are truly critical.

The current contingency analysis method can be viewed as an 'inside-out' approach. This is similar to looking at a complex machine element-by-element and identifying the impact of the failure of specific components. The alternative approach proposed here involves investigating the grid as a complete system and identifying combinations of elements which can lead to failure. This is akin to an 'outside-in' approach to grid reliability.

5.2 Challenges of Contingency Analysis

The technical challenge of contingency analysis is combinatorial. The total number of combinations of scenarios to be evaluated to exhaust all contingencies is a product of;

- the number of potential load sets (conditioned on time of day and seasonality),
- the number of possible generator failures (conditioned on make, age and maintenance policy of equipment),
- the number of control element failures (e.g. circuit breakers), and
- and the number of possible transmission element failures (conditioned on seasonality and age of equipment),

occurring with all possible sequences and timings that would result in coupled behaviors. There are too many combinations of initiating failures, load sets, and response performance options to fully evaluate for the nationwide power grid, or even a regional grid, using the most accurate power flow models. The highly non-linear and dynamic nature of power grid failure events (e.g. voltage collapse [11]) makes any linear simplifications of the problem to improve computational performance unproductive. So sophisticated analysis techniques have been developed to provide the insight equivalent to fully enumerating all failure modes.

The response time requirements for contingency analysis techniques depend upon the business process being supported. Near-real-time response is needed to support on-line

security assessment [10], whereas planning and evaluation functions can be performed off-line.

There are several approaches to managing the combinatorial explosion of contingencies for large power grids:

- **Simplifying assumptions** can be made to reduce the number of contingencies and the level of computer processing necessary to evaluate each contingency.
- Certain contingencies can be ignored after a computationally simple prescreening of the potential contingency list. This prescreening can involve many stages, with each stage representing more accurate, but more computationally intensive criteria. This is the basis of **state enumeration ranking and screening** approaches described below.
- An **adaptive** screening scheme can be employed, where later (in the list) contingencies are rejected based upon the results of full evaluations of earlier (in the list) contingencies. By cleverly ordering the contingency list, the chances for rejecting contingencies without full evaluation can be maximized. These are adaptive versions of ranking and screening.
- A statistical sample of the contingency list can be chosen to represent the entire contingency list developed using **Monte Carlo** techniques.

A brief look at each of these schemes is provided below.

5.2.1 Reducing the Contingency Set – Simplifying Assumptions

These simplifying assumptions are widely used in practice [6]:

- ***a priori* screening based upon the perceived likelihood of the contingency and load set**. These likelihood judgments reflect the historical experience of the portion of the grid under investigation, and are based upon expert judgment of the analysts. For example, in composite analysis, generation contingencies are generally reflected in much greater depth than transmission contingencies, since they are more common in practice. In practice, there is also some attempt to choose credible contingencies that are considered by the analyst, based upon historical evidence or expert judgment, to most significantly stress the performance of the network. This screening criteria is sometimes documented in network management guides for utilities or utility coordination consortia.
- I**gnoring the age and model of equipment** and instead using generic reliability and failure values for the type of power equipment.
- Removing duplicative runs resulting from **multiple identical machines in the same generating plant**. A single representative failure of a machine then represents the failure of any of the identical units.
- Manually flagging and deleting contingencies that are known *a priori* to be unimportant; this is known as determining the **importance based upon expert opinion, historical evidence or past analyses**.

- S**implifying the modeling of how control devices, reconfiguration, load curtailment and redispatch policies operate;** this reduces the number of possible control scenarios and control failure scenarios. The time dimension increases the number of contingencies that must be evaluated. Depending on the lag in the response of certain control devices, the combination of devices that must coordinate to manage the contingency, and the potential failure of those devices, the impact of the contingency can become increasingly severe and widespread. The evaluation of such conditions results in an explosion of possible combinations of event trajectories. Certain assumptions regarding the nature of the contingency and the response times of devices can be used to implicitly screen and reduce the number of contingencies that must be evaluated. This allows some consideration of control strategies while reducing the number of contingencies [12].
- **Reducing the scope of the network being studied** will reduce computation and analysis across all strategies**.** If the network to be studied is made smaller, fewer contingencies and less computational effort to analyze any given contingency is required. Much work has been done to develop simple models of external networks that interface with, but are external to, a study network, also known as **equivalencing** [13-16]. For a given contingency, the identification of a relevant impacted subnetwork to reduce analysis computation is known as **bounding** and is discussed in greater depth below.

Once initial scoping and simplifying assumptions are made, computational feasibility can be achieved with a balance of

- strategies to **reduce the size of the contingency set which is evaluated**, and
- strategies to **reduce the evaluation time each contingency of that set requires**.

Both of these strategic areas benefit from **improvement in system performance indices**. These three areas make up the bulk of contingency analysis research, and each is discussed below.

5.2.2 Reducing the Contingency Set - Implementation

Once modeling assumptions have been made, there have been four different strategies proposed for reducing the size of the resulting contingency set.

1 The first is to rank order or screen the potential scenarios based upon some sort of preliminary criteria (**state enumeration**).

2 The second is to randomly sample from the potential scenario population until the sample is representative of the entire suite of potential contingencies (**Monte Carlo**).

These are the oldest and most popular, and will be described in greater depth below.

State enumeration

Under state enumeration, for what are referred to as [n-1] contingencies, each major component of the power system is assumed to fail independently and to be restored

before any other system component fails. The evaluation of each of these potential failures is explicitly considered. The system performance under each single failure is assessed, and failure or success of the network under that contingency is determined. The key distinguishing factor of state enumeration is that **the contingency set is predefined before any performance assessment is performed.**

With deeper (i.e. [n-2], [n-3], etc. contingencies) contingency analysis, simultaneous failures are considered. Pairs, triples, etc. of components are assumed to fail, with common mode failures or historically significant past combinations of failures manually identified. Scenarios where remediation or protection systems fail are also considered. Because every member of the contingency set is potentially evaluated, the number of possibilities is constrained by the modeling and computational burden of assessing performance of each member. Performance is measured by the degree of system compromise or outright inability to satisfy demand (e.g. load commitment).

There are three techniques that fall under state enumeration for reducing the size of the contingency set: **screening, ranking,** and **optimization.**

State enumeration – Screening: Under screening, a simplified performance assessment model is used to identify which contingencies are candidates for the contingency set. Screening is based upon systematically testing contingencies and classifying them as either manageable, failures, or requiring further screening or evaluation. The two elements of screening are the systematic test process itself, and the criteria used to classify the contingency.

There are two basic levels of screening that are always applied in contingency analysis:

- at the beginning, when certain contingencies are considered too unlikely for consideration;
- at the end, when a performance assessment model is applied to the contingency and the results are assessed.

Since there is a hierarchy of performance assessment tools, with increasing computational burden but increasing fidelity, these tools in combination provide a sort of **hierarchical screening**. Coarser, faster models provide earlier screening.

- Some procedures exploit **previous solutions of contingencies to accelerate current calculations**. Intermediate computationally expensive steps, such as matrix inversions in power flow calculations, can exploit previous matrix calculations [17, 18]. This idea can be generalized **to reuse contingency analyses performed in past years** (or in past hours, for real-time evaluations) to accelerate computation [19].
- **Statistical regression,** where a response surface estimator of the full performance assessment model is developed from a regression model from previous contingency analyses, provides an even simpler performance assessment model. [20] **Pattern recognition** models provide a similar capability [21].

The challenge with this approach is to achieve a **powerful enough test** at each level using relatively crude tools [22]. This would involve both revising the performance indices and determining their use in a richer characterization than the accept/reject

classification of a simple bound. Based upon the results from these models, slower, more refined models are applied to refine interesting cases. Since the definition of "interesting" may be determined in part on the actual result, there is some iterative manual review as part of this process. The main challenge is the classic one of **maximizing the power of the test** based on the index, i.e. minimizing Type I and Type II errors resulting from either rejecting contingencies that are important ("masking") or including contingencies that aren't important. There is surprisingly little reference to the formal design of indices to maximize the power of the statistical test for which they are used. On a related note, **fuzzy logic** has been proposed to provide "degrees of confidence" in the security categorization of states [21, 23-25].

There are also cases where additional screening can be performed based on the results of full performance assessment for prior contingency sets. If, say, contingency A can be determined *a priori* to be less severe than contingency B, then if contingency B passes the performance assessment, contingency A passes as well. This is an example of **dominance** relationships that are identified after initial screening, but prior to actual performance assessment, and provide the basis for what can be considered an **adaptive screening** procedure.

State enumeration – Ranking: Ranking, or rank-ordering is simply imposing an extreme dominance relationship on potential scenarios (i.e. a strict ordering rather than partial ordering). All contingencies are assigned a place in a list and contingencies are sequentially analyzed from the top of the list until they no longer result in violation, whereupon the remaining contingencies are considered acceptable. A set of different rankings can be developed from a set of different performance indices (e.g. overload v. voltage collapse). Although intuitively appealing, there are known problems with this approach, since the impact of any error in the statistical test (e.g. "masking") is amplified under rank-ordering. Requiring a number of consecutive successes or failures before accepting or rejecting the remaining contingencies mitigates such effects.

State enumeration – Optimization: Since the set of potential contingencies is enumerated up-front, the problem of selecting those scenarios most worthy of continued analysis can be formulated as a non-linear integer programming problem under some worth function. The feasible region is the enumerated set of potential contingencies, and the objective is to select those contingencies that are the worst performers, according to some index value. This is more formally known as delta optimality. The same general techniques applied to non-linear integer programs have been proposed for contingency analysis. In recent years, research on such problems has focused on techniques in evolutionary computation such as evolutionary programming, genetic programming and particle swarm optimization. These techniques use biological analogies to develop robust heuristics to solve general classes of integer programming problems.

Genetic programming is a structured search technique that performs well across a broad range of problems, and has been proposed for studying voltage collapse contingencies [26] and the more general problem of planning distributed generation facilities [27]. A fitness function is used to screen candidate solutions, and new solutions are generated based upon a systematic perturbation from the most promising solutions. Since genetic programming naturally provides a set of good answers, rather than a single answer, it is a good fit for this problem. As a heuristic, it is not always perfect, but is correct in some

probabilistic sense. **Evolutionary programming** is more general but quite similar in approach, and has been studied for use in reactive power planning under contingencies [28].

Simulated annealing, another heuristic based upon a metallurgical rather than a biological analogy, has been proposed to address the VAR planning problem, which is closely related to the contingency analysis problem [29].

Particle swarm optimization flourishes in a Multiple Instruction/Multiple Data (MIMD) parallel programming environment. Multiple searchers explore the feasible region, and communicate among themselves as well as gather information on the surrounding region in contingency space to optimize performance measures. An example minimizing power loss by intelligent reactive power and voltage control is presented in [30]. More generally, **multi-agent based approaches** have also been proposed to address the general problem of optimal response to minimize system costs [10].

Monte Carlo Analysis

Under state enumeration ([n-1] contingency), each major component of the power system is assumed to fail independently and is restored before any other system component fails. The evaluation of each of these potential single element failures is explicitly considered. Under **Monte Carlo analysis**, statistically representative contingencies are selected based upon some probabilistic characterization of causal factors.

The Monte Carlo technique happens to normally involve more computation than state enumeration, but also reflects many more failure scenarios. Monte Carlo is used in practice to get a sense of the *width* of the contingency space, including issues such as weather dependence, load statistics, scheduling and dispatch strategies, and generator maintenance, while state enumeration plumbs the *depth* of all the contingencies for a specific set of preconditions [6]. Consistent with the idea of maximizing width, the level of detail in modeling the network is generally lower in Monte Carlo than in state enumeration.

Another major differentiator between Monte Carlo and state enumeration is how they capture the dynamics of failures and remediation processes. Under state enumeration, performance assessment models are static models: the sequence and timing of failure events are ignored. It is convenient under Monte Carlo to treat the occurrence of failures as **dynamic** with a blocked-event simulation approach where, say, failure events enter a queue with arrival rates determined by failure rates and service times by remediation times. The timing of events can be represented probabilistically with every Monte Carlo realization representing a new sample of failure modes, service rates, and inter-arrival times, thereby providing a more accurate characterization of the likelihood and effect of simultaneous failure modes and/or network degradation states.

Standard acceleration techniques for Monte Carlo simulation (e.g. **stratified sampling**) are applicable for these Monte Carlo runs, though they are not explicitly discussed in the literature.

Other Set Reduction Techniques

It is also possible to screen and identify relevant contingencies by **studying the results from analyses or models optimizing planning and operations**, where the contingencies which are poorly served are implicitly identified in the **optimal remediation strategy** solution [19, 28, 30-35]. In the case of determining optimal power flows, the decision variables for such models are **optimal commitment and dispatch** [31,32,34,35]. Some models include **optimal control logic** as part of remediation actions [28,30,33,36], including the application of **Petri nets** to identify the impact of distribution network contingencies [37]. Others include the **optimal deployment of VAR sources** [27,29] and **transmission capacity** [38].

It is also possible to work the contingency analysis problem backwards. The **final outage states could be enumerated *a priori*, and the process worked backwards as an inverse problem** to identify what sort of contingencies could lead to that outage state. Undesired network conditions are derived as part of the calculation of the system margin performance index, but the conditions are not used as the starting point to enumerate all the ways a network could enter into those states. These unacceptable operating point regions are characterized in terms of ranges of critical parameters that lead to those conditions. The suite of possible events that lead to critical parameters entering into these regions could be enumerated. Theoretically, a complete characterization of events that lead to unacceptable operations would be enumerated, and no event that led to acceptable performance would be generated. This reflects the common practice of using historical failure events that led to major outages as a touchstone for contingency analyses in individual utilities, guaranteeing that those sorts of outages 'never happen again.

Some researchers have described methods that are combinations of various tricks and techniques described above [39]. There has been no formal design exercise to combine these techniques in some system-optimal contingency methodology.

5.3 Computational Issues

Evaluating each contingency to the fullest possible extent is not necessary in order to provide the insight expected out of a contingency analysis. There are continuums of models that provide increasing fidelity at the expense of increasing computational time. Coupling the right level of fidelity with techniques to reduce the size of the contingency set can provide the needed insight at the least computational expense.

Contingency analyses use direct method and indirect method approaches [30]. Direct method approaches formally calculate the post-contingency power flows and bus voltages using various power flow models. Indirect approaches calculate system-wide performance indices directly, without a full formal power flow model. Indirect approaches are generally faster and are associated with ranking, since a single numeric measure of performance is immediately available, but their greater inaccuracy leads to more frequent and severe errors during the ranking procedures.

- The most commonly considered simplification of models is based on increasingly accurate modeling of the power flow (e.g. network flow models, DC models, or

early iterations of an AC flow model as contrasted against fully-convergent AC model or QSS simulation) [17, 40-43].

- To capture failure modes with faster dynamics, such as voltage collapse, increasingly dynamic load flow models provide another range of simplification. The more static the analysis, the cheaper the computation. Coupling relatively static models with quickly computed look-ahead measures of load-flow convergence can provide computational advantages [44-48].
- Since contingency analysis is a perturbation method, first-order or gradient information can be directly used to develop screens or orderings. [47, 49-52]. The gradient information is also captured in the matrices from the Newton-Raphson technique used to solve various power flow models. These first-order methods can be problematic, especially when considering voltage instabilities [11, 53]. Second-order information can also be exploited [18, 47]. Clever matrix algebra including factorizations and sparse matrix representations have been used to optimize computational performance for the general power flow problems and contingency assessments in particular [54].
- Since assessment of contingencies hinge on those portions of the network where there are voltage mismatches, overloads, etc., spending the bulk of the computational effort where mismatches seem to be arising (i.e. localization) can reduce the computational burden [12, 39, 51, 55-58]. Efficient bounding [42, 51, 54, 55, 59, 60] is the best known of these techniques, where the boundary of the subnetwork affected by a contingency is iteratively determined using network conservation principles in power and angle spaces.
- Alternatively, increasing refined assumptions on the performance of the grid (e.g. load at a load point independent of voltage, limited representation of remediation strategies [6], localization of effects of some contingencies [39, 45] and others [61]) can also accelerate the convergence of the models. These assumptions can be refined, in analogy to the hierarchy of power flow models described above, if early analysis suggests this is an important or interesting contingency.

One computational trick is applicable across all of the strategies. Because the suite of contingencies is known prior to the start of power flow simulations, it is possible to **exploit earlier results to accelerate convergence in subsequent runs**. For example, the solution to an earlier contingency power flow run can be used as the initial point for an iterative power flow solution algorithm for another contingency. This is also an option, to a more limited degree, in Monte Carlo. This general idea can be exploited, to varying degrees, in the methods described above. This provides a comparative advantage to those techniques that incrementally move around the failure space as opposed to genetic approaches that bounce around the failure space more quickly.

Some researchers have focused on how contingency analysis may be modified to **parallelize** well or are generally amenable to distributed computing [10, 39, 63-66]. The benefits from designs to exploit parallel computation compete against the benefits of clever serial schemes, such as reuse of earlier computations as a starting point for a new power flow solution.

5.4 System Performance Indices

All formal contingency assessments involve comparing a single index, or multiple indices, against some simple numeric standard. As noted previously, these standards are based on failure criteria such as capacity deficiency, line overload, system separation with load loss, bus isolation with load loss, etc. These performance indices can themselves be the direct product of a contingency analysis model, without any intermediate derivation of more precise information such as power flow calculations, at the expense of precision and accuracy. Indices that **avoid full power flow calculations to determine post-contingency voltage levels at each bus** have shown promise in reducing computation time while still supporting ranking and screening procedures [41, 67-70].

Developing new indices is the focus of active publication and continuing debate to support any of the contingency methodologies [41, 71-75]. The development of specific functional forms of indices to assess fragility or acceptability of systems is an important part of this research. Much of the recent work has focused on development of indices, and metrics on these indices, to address fast dynamic failure modes such as voltage collapse [75-78] and frequency stability [79].

When a single value such as an index is insufficient, another approach is to *a priori* determine "regions of instability" for multidimensional indices in state space. Here, two or more state variables are used in the same fashion as indices, and the boundaries between acceptable and unacceptable behavior form regions with curved boundaries. For voltage stability, for example, PVar and PW are two popular state variables. An excursion of the network into these instability regions, as characterized by local PVar and PW measures, would constitute grounds for further detailed analysis. Since the explicit modeling of system dynamics is so difficult and computationally expensive, a **margin** or safety factor is applied to indices that capture voltage and frequency stability failure modes. The design of such margins to support contingency analysis is a research challenge [80].

Generally, voltage stability analyses use a **system load margin** index [45, 80-82]. A collapse point is characterized as the minimum of a parabolic curve of bus voltage against load, so that estimating what the PV curve looks like for contingencies provides estimates of the collapse point and thus the margin between current operations and collapse. The challenge is to determine the nose of the PV curve and how it changes under specific contingencies. **Optimization** techniques have been used to calculate the optimal residual load carrying capability and use this measure as a performance index [36,83]. More simply, **eigenvalues**, which capture at some level the dynamic stability of the power flow, may be used in screening and ranking [47, 48, 84]. Stability indices based upon a **Fourier analysis of the impulse response of power network** (e.g. the signal energy of the network impulse response) have also been proposed to determine these collapse points more efficiently [85].

Voltage collapse events are inherently dynamic, whereas most practical evaluation techniques are static or quasi-static. **Coupling both static and dynamic models** to evaluate the dynamic voltage stability has been proposed [48]. Others have made indices **reflect possible near-future states more directly**, rather than reflecting a static view of

current stability [44, 80]. Ultimately, the development of indices of dynamic stability is more of a heuristic art than science, and comparisons of rankings and screenings on test and actual systems are used to argue the relative value of proposed indices – a good example is [79].

There has been some work looking at applying formal **risk** indices (i.e. probability x consequence) for ranking and screening [23, 86-89]. The likelihoods of individual contingencies are estimated and an expected consequence measure is used for ranking and screening. The benefit of a risk-based approach is that undue computational attention would not be spent on very rare, high-consequence events that would be rejected by engineers and analysts anyway.

Measures that reflect the difficulty in correcting a given contingency (known as **correctibility**), rather than inability to service load or distance from instability for such a contingency, have been proposed [90, 91].

Some **formal expert-based and AI approaches to design such indices** have been proposed [56, 92- 97]. The strength of such techniques is speed, transparency, and consistency for real-time applications. Hybridization of these techniques with conventional numerical calculations enhances the accuracy of the results at the expense of computational time that may not be available in real-time applications. They may also be useful in supporting more physically-based analyses based on power flow.

Neural networks (nets) are trained to identify patterns, such as what characteristics of contingencies lead to service failure, and can be thought of as an adaptive extension of regular indices [16, 63, 98-104]. Regular indices have a set of contributing terms that are combined to provide a single number. The weightings of these terms are static for normal indices, are optimally tuned in a couple extensions [22,105], and are fully adaptive in neural nets. The advantage of neural nets is efficiency and consistency in analysis results. These nets are designed to accept as input those variables that prove most predictive of ultimate system failure under contingencies. For contingency analysis, neural nets have been found to be slow in learning and to be highly sensitive to the set of solutions used for training. Other pattern recognition techniques [21, 24] have also been developed.

5.5 Other Contingency Analysis Issues

There have been **expert systems** and **visualization techniques** developed to support human prescreening of contingencies [106, 107]. Such techniques change the nature of the human decision process itself, rather than just providing a new set of numbers to an existing process. There is general research in how to integrate such techniques into decisionmaking processes, for example [108], but no research in the area specific to the problem of contingency analysis.

5.6 Summary

In the mid 1980's, a review of computer codes found that contingency ranking and deleting rare event contingencies that were two methods that were commonly used to reduce the run times of contingency analyses [109].

A more recent EPRI survey in the late 1980s reported that there is a wide disparity of techniques used in practice for evaluating the reliability and robustness of composite generation and transmission systems [6]. Some use advanced probabilistic techniques to evaluate multiple contingencies while some evaluate a deterministic set of contingencies. Internal and external performance standards for utilities are generally stated in terms of meeting a particular performance level during a failure of a specific nature or contingency level. There have been no additional requirements placed on U.S. utilities from a NERC standpoint to require any more formal methodology to be applied at the utility or regional level. Even in the late 1980s, however, there was a perceived need to develop contingency analysis systems that better reflected the effects of distributed generation and load management.

There have been no reported objective assessments of contingency analysis techniques (in the sense of calibrating results against actual network events). Since it is unlikely that an actual testbed for power grid failures can be built to objectively validate these models, the best we can do is cross-validate among the models themselves. There was some early work comparing techniques for on-line analysis [21] and a recent paper suggested some sophisticated assessment and comparison of techniques were performed at a utility level in France [54]. The lack of systematic validation and verification of contingency analyses from the US research community is surprising, given the relative stability of the U.S. power grid on which to base such analyses.

In research articles, performance measures for such methodologies include the speed of execution, the completeness of the characterization of the methods, and the accuracy of the characterization. Normally these techniques are demonstrated on the small IEEE Reliability Test System (RTS) networks, and perhaps one larger example from an actual power grid. The research focus is on the *potential* of these techniques to provide performance improvement on this now-classic problem, not on actual assessment of whether these techniques provide such improvement in practice. One indicator of this state of affairs is the lack, with one exception [95], of any research to formally design a process that combines several of these techniques.

Surprisingly, there is a published comparison between the two popular power grid analysis programs, COMREL and TRELSS [110]. There was a disheartening lack of agreement between the contingency analysis solutions of the two codes. The desire to differentiate themselves based upon unique features makes it difficult to compare each code's handling of remedial action, for example.

No large integrated system has quite the combination of size, tight coupling, highly non-linear dynamics and short time constants as electric power. Telecommunications systems face similar problems but have had (prior to packet networks) more predictable linear response. There is also little chance of hardware damage from any flow-related failure mode in a telecommunications network. A 1990 study of the robustness of the US telecommunications network included relatively few manually defined scenarios [92, 93]. The lessons learned and techniques developed in power grid contingency analysis will be relevant as other infrastructures operate in a tighter, more non-linear fashion. In summary:

- There is a whole suite of theoretical approaches to the problem of contingency analysis.
- None of these techniques has been evaluated well enough to determine their relative benefits and costs.
- Few sophisticated techniques have made their way into practice.
- There has been no attempt to design an efficient process exploiting a combination of these theoretical approaches.
- In spite of the limited penetration of some of the more sophisticated techniques, power contingency analysis is more advanced and formalized than the equivalent techniques for other infrastructures.

6.0 Node Identification

6.1 Disruption of the System

Contingencies are defined as potentially harmful disturbances for the steady state operation of an electrical network. A contingency may comprise the loss of any combination of network elements. Disruption or failure of a single element in a power grid is called a single point contingency, a first-order contingency or generally, simply a contingency. Contingency analysis is basically a perturbation analysis on existing power flow analytic and simulation models and is conducted with the express purpose of identifying whether an electric power system will perform acceptably when individual components of the system fail or are disrupted in some manner. The non-linear behavior of power networks and rapid propagation of failure events makes formal contingency analysis critically important. These same nonlinearities, coupled with the size of the network and the uncertain nature of demands and environmental conditions, makes modeling to support contingency analysis particularly difficult. Normally, there is a policy in place at the utility or control region level to ensure no contingencies of a particular type or likelihood will compromise the system to a certain level.

This research focuses on what is known as composite system reliability, considering failures in both the generation and transmission. Both the PFLOW and IPF computer models (discussed below) assess the adequacy of a specific power grid configuration (generation and transmission) to meet a forecast load set. The technical objective is to identify all those contingencies that result in system failure or compromise at some level, and ensure none of the relevant contingencies are in this set.

The fundamental mathematical characteristics of a bulk power vulnerability analysis includes:

a. A system described by a space of possible network elements that can be disrupted: $E = \{e_i\}$.

b. A cost function f on E, which maps the disruption of the network into a set of values $E \xrightarrow{f} C = \{c_i\}$, which characterizes the impact of disrupting the network.

c. An order on C, so that for every pair of elements of C (c_i, c_j), we can say we have either $c_i < c_j$ or $c_i \geq c_j$.

6.1.1 System Definition

For the current discussion, the set of possible network elements, E, has been limited to generators, transmission lines, substations and transformers. Of specific interest are those elements associated with bulk power networks. While there is no consistent definition of what constitutes a 'bulk power network', the definition established by NERC refers to that portion of an electric utility system, which encompasses the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Alternatively, some

organizations have established definitions which are 'performance based' and as such do not include reference to a particular voltage level. For example, the 2001 National Energy Policy definition is performance based and is taken to encompass all the facilities and control systems necessary for operating an interconnecting transmission grid (or any portion thereof), including high-voltage transmission lines; substations; control centers; communications; data; operations planning facilities; and the output of generating units necessary to maintain transmission system reliability. The definition does not refer to a particular voltage level; however, in general, a bulk power system is assumed to subsume power grid components associated with the generation and transmission of 69 – 141kV.

6.1.2 Performance Measures

Before we can discuss the identification of critical network elements, it is necessary to understand what is meant by 'critical'. A power grid element is considered critical if, in the event of a loss of that element, a significant negative change in power grid performance is expected. This negative change in power flow capabilities is ***initially*** exhibited through the increase in branch loadings in excess of 100% of the branch rating either in current or voltage. The use of line or branch ratings to characterize a particular power flow network configuration is common practice in the power industry. However, for our analyses a single valued performance measure is required. A number of simple performance measures have been developed based on line ratings. The most basic is simply a sum of the branch loadings in excess of 100%, while a variation on this accounts for the line capacity as well the line overloading.

The general procedure begins with the construction of a fundamental, base case load flow analysis and a check for convergence. After convergence each of the buses is examined to make sure that the sum of real and reactive power is close to zero. Any existing mismatches are required to be a very small percentage of the power available at the bus. After confirming convergence to an acceptable solution, the line ratings are observed to determine that all transmission lines are operating within allowable current and/or voltage ratings. Those lines that exceed specification are then identified; of particular concern are those lines exceeding approximately 69kV since the impact will be less localized. For the preliminary assessment it is assumed that any line exceeding a specified level (e.g. 110% of the normal rating) will be removed from service either manually or automatically. The 110% criteria is a bit arbitrary since the actual criticality point varies from utility to utility ranging from 100-115%; however, it is felt that it represents a reasonable indication of a significant power system problem.

6.2 Complex Network Theory

6.2.1 Background

Network theory has been applied extensively on a wider variety of complex networks including communication networks, the Internet, and even power systems. The goal of these efforts has been to characterize the robustness, fragility and attack tolerance of complex networks. Large networks can be typically classified into two groups: homogeneous and non-homogeneous. Nodes in homogeneous networks typically have

roughly the same number of connections. Random graphs and small-world networks are examples of homogeneous networks.

The fundamental concepts around 'small-world' theory are analogous to the notion that surrounds the popular folklore of 'six-degrees of separation'. In 1967 a Harvard sociology professor Stanley Milgram [113] proposed an experiment in which a randomly chosen group of people in Omaha, Nebraska would, through a sequence of family, personal or professional contacts, deliver a message to a single final contact in Boston, Massachusetts. He found that the average number of contacts required was six, hence the reference to 'six-degrees of separation' and the idea that, while our social network is large and complex, it really is a 'small world' out there.

The notions of small-world theory were first proposed by Watts and Strogatz [114]. They suggested that networks describing many biological, social, and technological phenomena have certain structural characteristics that describe how the information element unique to that network (e.g. disease, power) is dynamically distributed through the network. These characteristics are the network path length L and clustering coefficient C. Small-world networks are characterized by a high degree of clustering and short path length.

The bulk power system in southern California has the appearances of a small-world network [115].

Scale-free networks are largely homogeneous, but contain a few nodes that are highly connected (Figure 4). The Internet and World Wide Web are examples of scale-free networks. Scale-free networks typically result from an evolving system with preferential points of interconnection. The Internet and the World Wide Web have such properties.

6.2.2 Network Theory Basics

The basic constructs of network theory are a collection of vertices and the edges that connect them. The graphs considered here are assumed to be complete or fully connected with every vertex reachable from any other vertex with a finite number of steps. The edges are unidirectional and unweighted; multiple edges between vertices are not allowed.

Let $W = \{w_i\}$ be a set of nodes and let the set of edges between the nodes be $E = \left\{\varepsilon_{ij} = \{w_i, w_j\}\right\}$, where $\varepsilon_{ij} = 1$ if nodes i and j are connected, $i = 1,...,n$, $j = 1,...,M$. These two sets then define a graph $\Omega = (W, E)$ with order n and size M where $M \le n(n-1)/2$. The minimum number of edges that must be traveled to get from node i to node j is the shortest path length between w_i and w_j and is defined as the distance $d(i,j)$. The number of edges attached to a vertex w is the degree of that vertex, k_w. The average degree over all vertices of a graph is $\langle k \rangle$ and $M = (n\langle k \rangle)/2$.

The characteristic path length, $L(W)$, is the median of the means of the shortest path lengths connecting each vertex to every other vertex. The diameter of a graph, D, is the length of the longest among all distances between any pair of vertices. The diameter provides a measure of the ease with which information flows between two vertices: the

smaller the diameter, the shorter the distance between vertices. Albert, et al. estimated the diameter of the World Wide Web as having a diameter of 19.

In addition to having small-world characteristics, the Internet and power grids have been shown to be scale-free [116]. This is evidenced by the frequency distribution of the number of connections on each node as given by a power law relationship: $P\{k\} = ck^{-a}$, $k = m, m+1, \ldots, K$, where m is the smallest number of connects at a node and K is a very large, possibly infinite number, (but can be estimated using $\sum_{i=K}^{N} P\{k\} = 1/N$, [117]).

Let the set of nearest neighbors to node w_i be defined as: $\Gamma_i = \{n_i \mid \varepsilon_{ij} = 1\}$, not including w_i and let $|E(\Gamma_w)|$ be the number of edges in the neighborhood of w_i. The clustering coefficient characterizes how closely related groups or clusters of nodes are related, and is expressed as:

$$C_w = \frac{|E(\Gamma_w)|}{\binom{k_w}{2}}$$

A network clustering coefficient $\langle C_w \rangle$ can be found by averaging over all vertices.

Computer algorithms for identifying shortest path, neighborhoods, etc. and subsequently network diameter and clustering coefficients are found in Cormen et al. [118].

6.2.3 Approach

Small-world and scale-free network theory were investigated as possible means to identify network weak points. The approach utilized to identify vulnerable points on the grid is similar to that first proposed by Albert, et al [119] and also by Cohen, et al.

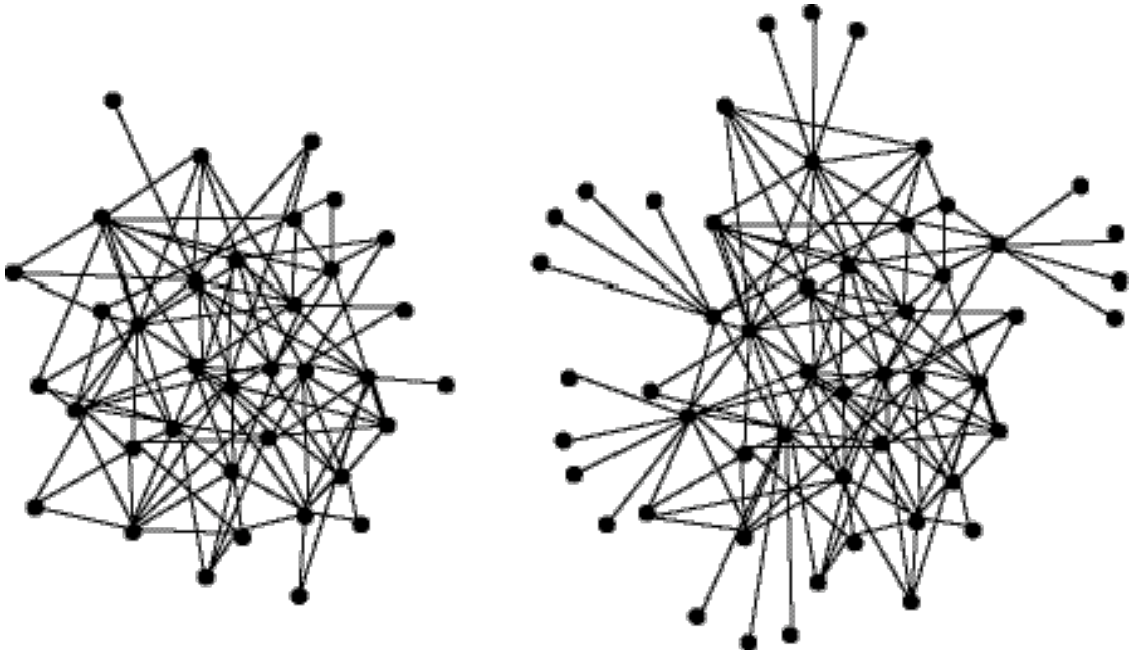


Figure 4: Examples of Homogeneous and Scale-Free Networks

[120,121].

The basic concept is that, for a network of connected nodes, if a fraction, p, of those nodes are removed, then the network will disintegrate into a set of minimally connected nodes. The degree of connectiveness of the network defines this critical fraction and this fraction in turn defines the resilience of the network to disruption (either intentional or random). The robustness (or inversely, the fragility) of a large network is characterized by its diameter, which is the average length of the shortest path between two nodes. The fragility of a network is investigated as nodes are removed and the diameter of the network changes.

6.2.2 Conclusion

Network theory was expected to provide interesting insight into the bulk power system since it had previously been used to characterize the fragility of such varied networks as the Internet and complex ecological systems. In addition, the techniques had been used to investigate a rather large bulk power system, the WECC, which serves the majority of the western United States [115].

As noted initially by Albert et al. [119] and subsequently by others, the analysis of networks using classic metrics (e.g. diameter and clustering) leads to the conclusion that complex networks such as the bulk power network and the Internet are robust to removal of a random selection of node combinations. According to current network theory, only a strategy focused on the targeting of highly connected nodes has been found to have an overall disruption impact on the network.

Unfortunately the recent events of 1996 and 2003 indicate that, in reality, the bulk power system is sensitive to the disruption of not only nodes with minimal connectivity, but multiple, single connected edges as well. This is contrary to the results of all network analyses published to date.

While an interesting theory for conversation, it does not seem to provide substantial additional information beyond what is available in the classic technique of polyhedral dynamics that was also investigated.

6.3 Polyhedral Dynamics

Polyhedral dynamics is a branch of set theory, introduced by Atkin in 1977 [122], that deals with the topological relationship between finite sets. q-analysis, in turn, is an algorithm used to study polyhedral dynamics. The two terms (q-analysis and polyhedral dynamics) are often used interchangeably. Cabral [123] applied the methodology to investigate complex tasks, and Casti [124] applied q-analysis to characterize the complexity of large systems. The underlying information structure in knowledge based systems as well as complex water infrastructures were investigated by Duckstein [125, 126]. Robinson and Duckstein [127] used polyhedral dynamics to identify the bottlenecks within a flexible manufacturing system.

In this particular application, polyhedral dynamics involves characterizing the bulk power system as a complex series of n-dimensional polyhedra, similar in many ways to a large crystal. The vulnerable points on the grid expose themselves as ‘cleavage’ points in the

crystalline structure. Polyhedral dynamics is employed to relate the various elements of the power network to a simplicial structure and to identify the vulnerable points in the network.

q-analysis describes the interconnectivity of *n*-dimensional polyhedra. Let $X = \{x_1,\ldots,x_m\}$ be a finite set and $Y = \{y_1,\ldots,y_n\}$ be a second set with some relationship with set *X*. The relationship between *X* and *Y*: $L \subset X \times Y$ is a binary relationship characterized by an $n \times m$ incidence matrix **A** where:

$$[a_{ij}] = \begin{cases} 1 & \text{if } x_i \text{ is } L\text{-related to } y_j \quad i = 1,\ldots,m;\ j = 1,\ldots,n \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

The relationship *L* can be defined as a threshold value where x_i and y_j are *L*-related if, for example, x_i and y_j are buses on a power grid and the power flow between them exceeds a particular value.

The incidence matrix **A** represents a simplicial complex composed of a set of *n*-dimensional polyhedra: $K_Y(X;L)$. A *simplex* is a spatial configuration of *n* dimensions determined by *n + 1* points in a space of dimension equal to or greater than *n*. A simplex may be a point coincident with a vertex, a line connecting two vertices and so on. A triangle described by three vertices from the set *X*, along with its interior, is a two-dimensional simplex in any space of dimension greater than or equal to *n*. The set *X* represents the vertices of these polyhedra, while the members of the set *Y* are associated with the edges or faces of the polyhedra.

Note that the construction of the conjugate complex, $K_X(Y;L)$, can also be very informative.

6.3.1 Example

Let $X = \{x_1,\ldots,x_6\}$ and $Y = \{y_1,\ldots,y_4\}$ with a relationship structure characterized by the relationships in Table 1.

Define a relationship such that $(x_i, y_j) \in L$ if and only if $[x_i, y_j] > 2$. Applying this threshold to the table at the right, the resulting incidence matrix **A** is then:

	y_1	y_2	y_3	y_4
x_1	1	5	3	2
x_2	3	4	7	1
x_3	4	2	4	1
x_4	1	3	6	2
x_5	2	1	2	5
x_6	1	2	0	4

Table 1: Relationships for Example 1

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Figure 5 depicts the resulting simplicial complex. Simplex y_1 is the line segment defined by the points $\{x_2, x_3\}$. The y_2 is the plane defined by the points $\{x_1, x_2, x_3\}$ while the y_3 simplex is the entire tetrahedron. Finally, the area inside the triangle $\{x_4, x_5, x_6\}$ defines the y_4 simplex.

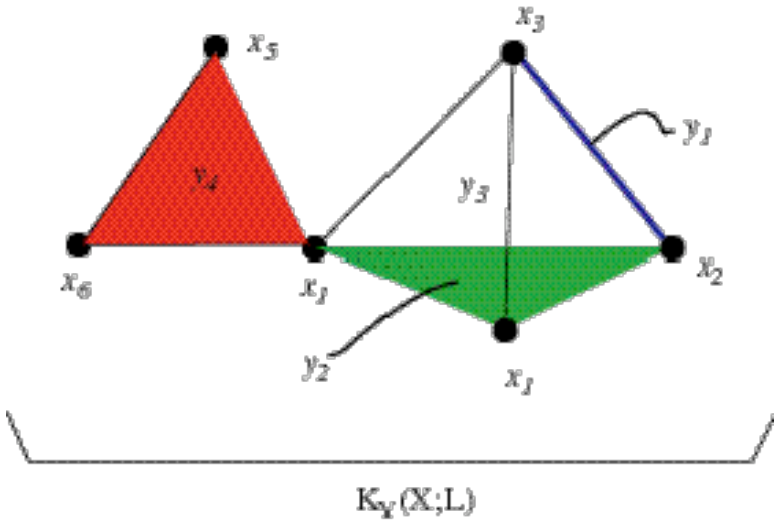


Figure 5: Simplicial Complex for Example 1

6.3.2 Simplicial relationships

There are various constructs that can be used to describe the relationships between the various simplices, σ_a, within the overall complex $K_Y(X;L)$. The most fundamental relationship involves the identification of groups or equivalent classes within the complex. In particular, it is informative to characterize how the various simplices within the complex are connected to each other. Simplices may be directly connected or connected through a series of other simplices.

Formally, two simplices, σ_a and σ_b, are connected if and only if there exists a finite sequence of simplices $\left[\sigma_{a_i}; i = 1,\ldots,p\right]$ such that: 1) σ_a is a face of σ_{a_i}, 2) σ_{a_p} is a face of σ_b, and finally 3) σ_{a_i} and $\sigma_{a_{i+1}}$ share a face of dimension d_i, where the dimension of the simplex is one less than the number of common vertices. The connectivity of two simplices is then: $q = \min[a, d_1, d_2, \ldots, d_{p-1}, b]$ where $q = 0,1,\ldots,N$,and N is the maximum simplicial dimension within the simplicial complex $K_Y(X;L)$.

Each degree of connectivity, *q,* has one or more groups or classes which share the same degree, and the number of classes at each degree q is Q_q. It is then possible to characterize the system in terms of the relationships between these equivalence classes. These classes are represented in vector form: $\mathbf{Q} = (Q_N, Q_{N-1}, \ldots, Q_0)$. This vector provides an indication of the interconnectivity among the different simplices. For example, a connectivity vector **Q**, composed primarily of low numbers, indicates a 'string' of low dimensional simplices with little connectivity, i.e. a loosely bonded structure susceptible to 'damage'. The connectivity vector also provides a qualitative window into the dynamic changes in system structure as disruptions are introduced (e.g. nodes removed) – hence the name polyhedral *dynamics*.

The connectivity vector **Q** provides a *qualitative* measure of the system connections. However, it is essential to *quantify* the strength or importance of the connections between the classes. A measure of the strength of the connection between one simplex and the other simplices is: $\varepsilon_i = \frac{q_i' - q_i^*}{1 + q_i^*}$, where q_i' is the dimension of the σ_i simplex and q_i^* is the largest degree of all the classes to which σ_i belongs (i.e. the maximum dimension of a face shared with another simplex). The smaller the value of ε_i, the more interconnected the simplex is with the other simplices. A value of $\varepsilon_i = \infty$ indicates that the simplex σ_i is not connected to any other simplex..

6.3.3 q-Analysis Algorithm

While the simplicial complex for the above example is rather simple to construct, Atkin (1977) provides a simple algorithm for performing a *q*-analysis of a system. Let **A** be the $n \times m$ incidence matrix. Then

a. Form $\mathbf{A}\mathbf{A}^T \quad (n \times n)$
b. Evaluate $\mathbf{A}\mathbf{A}^T - \mathbf{1}$ where **1** is an $n \times n$ matrix of 1's
c. Since the resulting matrix is symmetric, all the necessary information is in the upper triangular portion of the matrix. This, together with the main diagonal is referred to as the *shared face* matrix.
d. The main diagonal is the **Q** vector
e. Reading across a row or down a column associated with an element of **X** gives the connectivity of that element with other elements

6.3.4 Application

In this section a sample bulk power system is transformed into a simplicial complex. A software routine was written to automatically extract the incidence matrix **A** from a General Electric formatted power grid file. The resulting incidence matrix can then be used to construct the simplicial complexes and perform a *q*-analysis on the resulting structure. Critical network locations are then easily identified.

The analysis was applied to the IEEE 300 Bus reliability test system. The IEEE 300 system is actually composed of three interconnected subsystems. In Figure 6 the top four critical nodes for the entire network are identified with red stars overlaid on the network diagram. *q*-analysis also permits analysis on subnetworks. Using only the data from System 1, the top four critical nodes for this subnetwork are easily identified and are again highlighted as red stars overlaid on the System 1 subnetwork diagram in Figure 7.

6.3.5 Polyhedral Dynamics Summary

Vulnerability analysis using polyhedral dynamics is fast, simple to apply, and can be easily automated. Data sources such as the GE data formatted files are easily obtained for every power grid network in the United States, in many cases down to the local, distribution level. It certainly holds the possibility of quickly identifying critical nodes or elements where additional security measures should be investigated.

However, polyhedral dynamics is a topologically based analysis tool. It does not account for even simple power relationships that clearly exist in complex power networks.

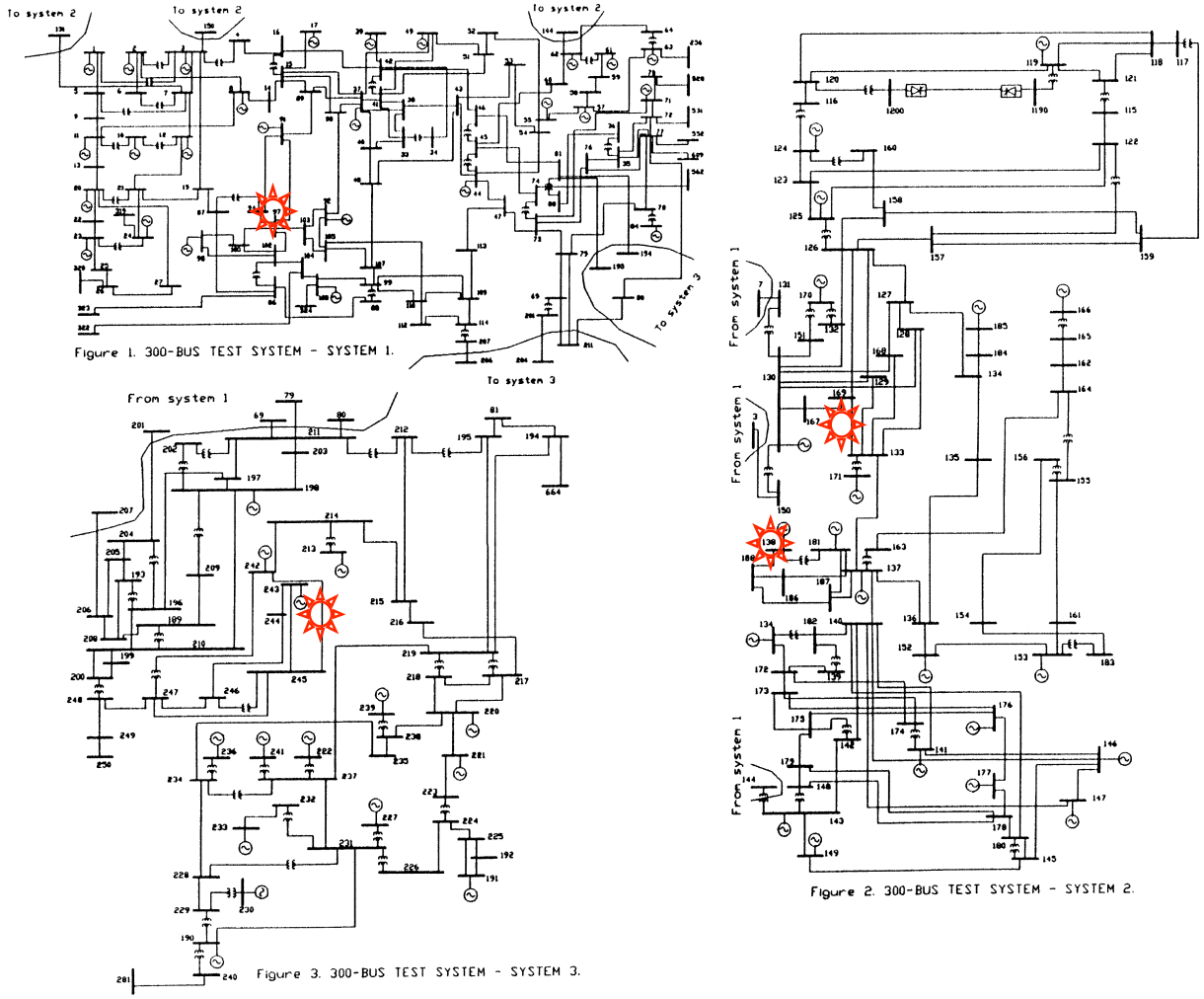


Figure 6: Critical Nodes for Complete IEEE 300 Bus Test System

Inherent within the paradigm is the assumption of independence between the failures of network elements that is captured in a static power grid analysis.

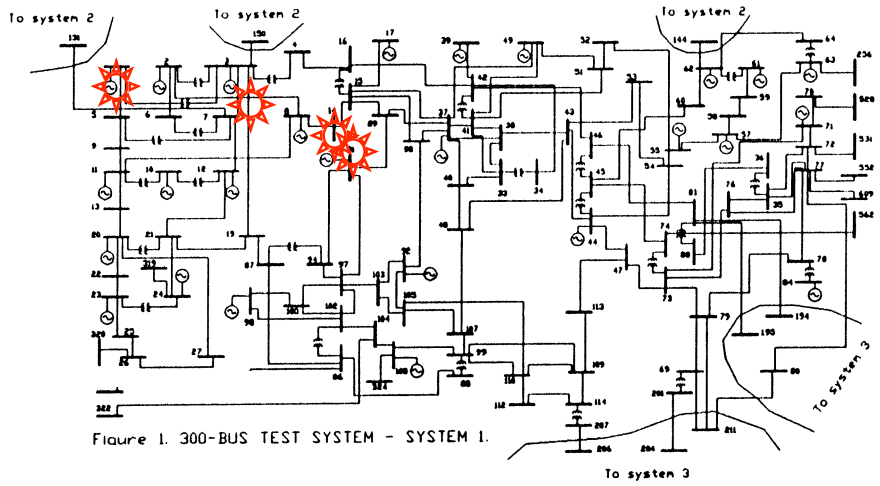


Figure 7: Critical Nodes for IEEE 300 Bus Test System – System 1 Only

6.4 Particle Swarms

The fundamental concepts associated with particle swarms were developed in 1995 by Kennedy and Eberhart [129, 137-140]. Particle swarm optimization (PSO) is regarded as being of the family of evolutionary strategies for problem solving. Other members of this family include, for example, genetic algorithms and evolutionary programming. While heavily influenced by the philosophy of evolutionary strategies, PSO differs significantly from these "survival of the fittest" algorithms in that it is based on a social cooperative perspective: individuals working with others in a common social group to solve problems. Contrary to the algorithms in Darwinism-based paradigms, individuals are not replaced by better performing individuals; rather, the individuals in a swarm model adapt to the environment by gathering information and processing that information as a group. In a swarm model it is not the individual who changes, but rather the knowledge of the individual that changes from iteration to iteration.

It should be noted that PSO is also closely related to the area of cellular automata, which is a discrete time, discrete state virtual machine where the current state of each cell of the system is determined by its most recent past and the states of those cells in the immediate proximity.

Since 1995 PSO has been used by a number of authors to address a wide variety of applications [131-136, 141] including optimization of reactive power and voltage control for a bulk power system [134, 144-145]. Swarm intelligence is particularly suited for our problem due to its evasion of local minima.

6.4.1 Background

As noted by Kennedy and Eberhart [140, p288], in a very simple sense an individual reacts and adapts to their environment, including other individuals, through three major principles: evaluating, comparing, and imitating. Individuals can identify desirable goals and objectives of their social group within the environment and have their own perception of their behavior relative to environment. They can also compare their behavior to the behavior of other individuals in achieving those goals and then imitate the behavior of those individuals who are seen as having behavior conducive to achieving those goals. By adapting in this fashion, individuals take advantage of the *experiences* of those individuals around them in much the same fashion as a school of fish takes advantage of the many eyes available to the group to warn of danger and the subsequent reaction of the group to avoid the danger.

Stepping quickly away from the metaphors, let an individual with a certain behavior set be described as a particle with a certain *position*. The change in the behavior of the individual as it seeks to imitate the behavior of successful individuals is characterized by the *velocity* of the particle.

A particle is distinguished by its:

- current position and velocity,
- value of that position,
- best position achieved thus far,
- best current position achieved by those particles in its neighborhood.

A swarm is characterized by a set of particles and one or more neighborhoods describing the social structures of those particles. Each particle in the swarm changes position and velocity through a combination of it own past best experiences as well as the best experiences of it neighbors. This ability to gain and gather *experiences* individually and from the neighborhood provides the individual particle with *memory*. This capacity for memory is important since it allows the algorithm to exploit information via a local search (through the experience of each individual) and it also emphasizes exploration of the search space with a global search (through the combined experiences of the neighboring particles). This balance of local exploitation and global exploration results in a very robust search algorithm.

The traditional swarm equations take the form [129]:

$$v_{i,t+1} = c_1 v_{i,t} + c_2(p_{i,t} - x_{i,t}) + c_3(p_{g,t} - x_{i,t}) \tag{1.1}$$

$$x_{i,t+1} = x_{i,t} + v_{i,t+1} \tag{1.2}$$

where:

$x_{i,t}; v_{i,t} \equiv$ position; velocity of particle i at time t

$p_{i,t} \equiv$ position of best performance of particle i through time t

$p_{g,t} \equiv$ position of best performance of $g$roup through time t

$c_i \equiv$ coefficients

The meaning behind each of the terms in the above equations will be discussed in the following section, but to tie this all together, let us use the example of a flock of birds. The specific objective of this 'social' group is to minimize the distance between themselves and a source of food (such as a cornfield). Utilizing equations 1.1 and 1.2 results in a series of positions as a function of time as the search progresses. Movie 1 depicts typical results.

Movie 1: Flock of Birds Foraging

6.4.2 Approach

In the following discussion, the analogy between a group of terrorists, a cell, and a swarm will be exploited. It is important to understand that the analogy results from a serendipitous situation and not from any attempt to actually model the social behavior of a group of terrorists. The algorithm operates quite distinctly from the analogy; however, the analogy provides a unique vehicle for discussion purposes.

In our application of a swarm paradigm the swarm will consist of a number of terrorists linked together into a loose social structure (i.e. a cell) with the goal of causing maximum disruption to the national bulk power system. A particle in the swarm will equate to a terrorist and a swarm neighborhood or social network will equate to a terrorist cell. Note that this can be generalized further in the sense of having a terrorist cell modeled as a member of a larger organization.

The 'position' of each terrorist is analogous to the choice of targets each terrorist has made from a long list of potential targets while 'the ''velocity' of each terrorist relates to the probability of the terrorist choosing a particular target. Each terrorist in the cell will have access to education, training and a variety of independent information sources. This knowledge base will be periodically queried and a decision on the suggested best course of action will be provided to the individuals. The phrase 'suggested' is used since there is a certain degree of interpretation and free will that lend uncertainty to the actual course of action taken by the individual antagonist.

In general, the position of the particle at a particular time is a continuous variable. However, in our situation, the positions $x_{i,t}, p_{i,t}, p_{g,t}$ can take on only binary values {0,1}. The individual best $p_{i,t}$ will take on values of 1 if the individual best performance occurred when position $x_{i,t} = 1$ and similarly, $p_{i,t}$ will take on values of 0 if the individual best performance occurred when position $x_{i,t} = 0$. Following the example of Kennedy and Eberhart [129], we will assume that the velocity $v_{i,t}$ represents the probability that the position takes a value of 1. The probability of the null position $x_{i,t} = 0$ is therefore $1 - v_{i,t}$. The change in position is then given by evaluating: if $(rand() < S(v_{i,t}))$ then $x_{i,t} = 1$; else $x_{i,t} = 0$.

The transform expression $S(v_{i,t}) = 1/\{1 + \exp(-a\, v_{i,t})\}$ is controlled by the slope parameter *a*, where the slope at the origin is *a*/4. Typically, from an application point of view, this sigmoid function is limited over the range $[-v_{\max}, v_{\max}]$ (Figure 8). This prevents the velocity from being driven to zero too quickly and forces exploration of new

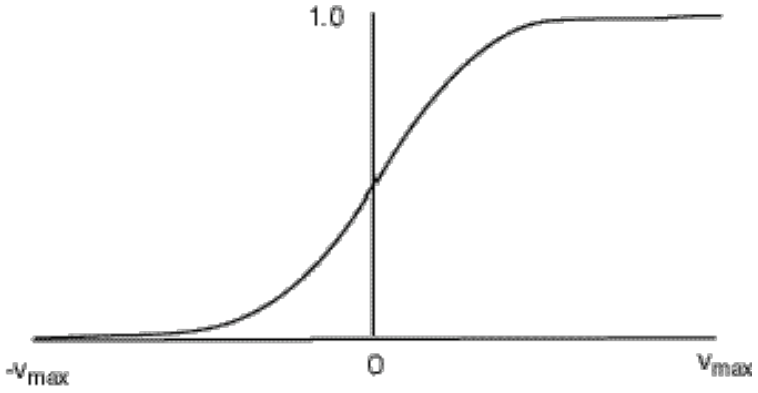


Figure 8: Sigmoid Function

positions.

With the above formulation, the analysis can proceed equally from two directions with the overall goal of causing as much damage as possible. First, we can take the perspective of the terrorist cell composed of individual terrorists. In this case, conceptually, the term $c_2(p_{i,t} - x_{i,t})$ represents the individual's contribution of knowledge to the overall objective of the terrorist cell. This knowledge may consist of such things as personal experience, unique training or specific educational background. On the other hand, the term $c_3(p_{g,t} - x_{i,t})$ represents the contribution of the individual terrorists

knowledge to the collective knowledge of the complete terrorist cell including the cell goals and objectives.

Alternatively, it is possible to formulate the problem as a terrorist organization with particular goals and objectives, $c_3(p_{g,t} - x_{i,t})$, composed of cells with their own unique knowledge base to draw upon, $c_2(p_{i,t} - x_{i,t})$. Finally, we can extend the velocity equation to account for all three levels of social dynamics:

$$v_{i,t+1} = c_1 v_{i,t} + c_2(p_{i,t} - x_{i,t}) + c_3(p_{g,t} - x_{i,t}) + c_4(p_{c,t} - x_{i,t}). \quad (1.3)$$

In all cases, the coefficients $c_j, (i \neq j)$represent the value placed on the level of contribution of each social segment (individual, cell or group) to achieving the objective. Typically the contribution level can change dynamically as knowledge is lost/gained/obscured in the course of the search for the optimum course of action. These coefficients are therefore treated as random variables that are re-evaluated at each stage of the analysis. Any alternative course of action is therefore a weighted average of the individual best course and the group best course of action: $\frac{c_1 p_i + c_2 p_g}{c_1 + c_2}$. The coefficient c_1 on the velocity term represents the momentum toward change in achieving the objective. In the simplest situation, the desire to achieve a particular goal or objective remains constant throughout the search for the best scenario. However, it is realistic to assume that this momentum may be greater the further away from the hoped for best solution and become smaller as the accumulation of individual and group knowledge

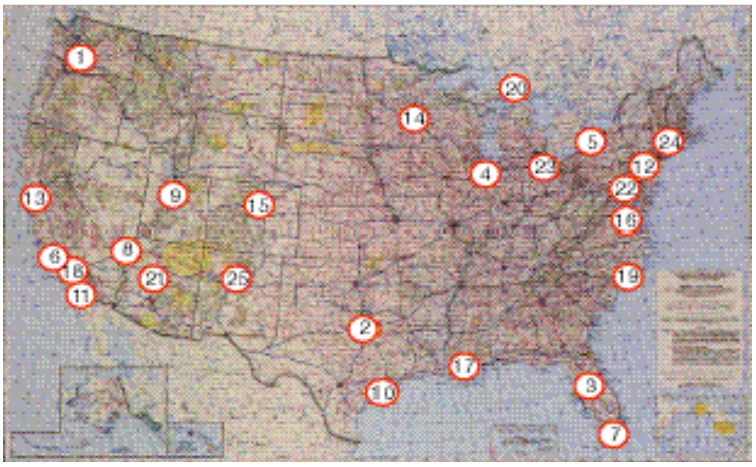
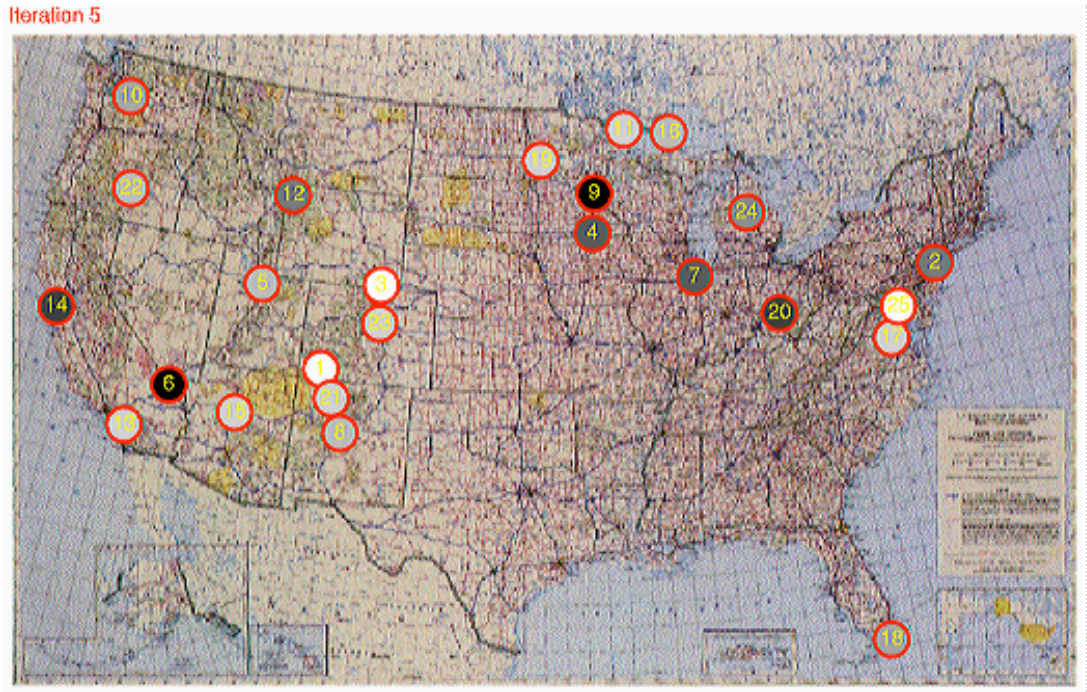


Figure 9: Target Designations for Simple Example

begins to focus the alternative courses of action into the one that best in achieves the objective.

6.4.3 Simple Example

In this very simple example, there are 25 potential targets available for destruction (see Figure 9). The destruction of each of these targets has value and these values are independent from each other. The cell consists of 10 terrorists gathering information



Movie 2: Target Selection: $p_{g,t}, t = 5,10,\ldots,150$

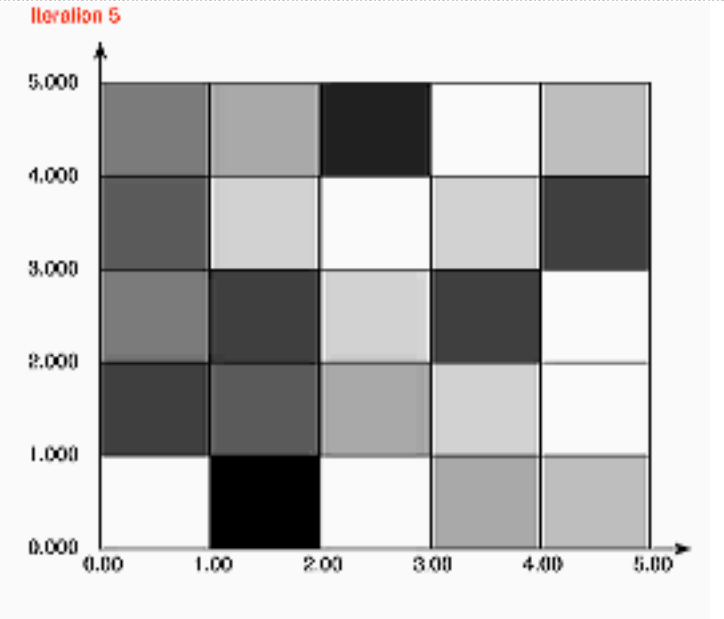
regarding the value of the possible destruction of these 25 potential targets. There are a limited number of resources available (people, weapons, explosives, etc.) which limits the number of targets destroyed to a maximum of four. An arbitrary 'value' for each target is given in Table 2, with higher values indicating more strategic importance, as one might expect.

The momentum is assumed to be constant (i.e. $c_1=1$), and the variables c_2 and c_3 are uniform random variables defined over the interval [0,2]. A total number of 40 iterations were explored before the program was terminated.

Movie 2 presents a movie of the group best positions, $p_{g,t}$, as they change for $t = 5$, 10,..,150. It is clear that the final top 5 targets, {3,6,8,20,22} are quickly identified in this simple example. This is not always the case since the search is stochastic in nature and

Target	Value	Target	Value	Target	Value	Target	Value	Target	Value
1	24	6	465	11	410	16	196	21	316
2	206	7	382	12	18	17	141	22	477
3	492	8	424	13	69	18	193	23	1
4	275	9	271	14	156	19	396	24	153
5	51	10	250	15	412	20	451	25	193

Table 2: Target Values for Simple Example



Movie 3: Grid Representation of Velocities

the existence of multiple solutions is possible in many bulk power systems. In general it is good practice to repeat the analysis and compare results.

Movie 3 also presents another interesting perspective on the search for the best targets and the final solution. In the movie, the shading represents the velocities associated with the group best positions as they change during the knowledge gathering process. Note that these velocities are presented prior to being transformed into probabilities by the sigmoid function so the velocities in the figure actually range over the interval [-3,3]. In general then, the figure represents the likelihood of a target being selected and the movie depicts how this probability changes as the search progresses. Targets with velocities in the neighborhood of –3 have probabilities close to 0.0474 of being chosen for destruction (white in color), while targets with velocities at the other end of the scale, +3, have a probability of 0.9526 of being chosen (black in color).

The presentation of target selection likelihood is rather simple in the small size suite of targets used here (25). As the number of targets increases, presentation will be more difficult. An alternative mode of presentation will therefore be utilized at times in which the likelihood will be presented as a 2-dimensional image where lighter pixels are targets that are more likely to be selected. Movie 3 is a movie that depicts as a 5x5 image the changes in likelihood of target selection as the search for the best target combination transpires.

Note that it is quite simple to change the value structure from a one-dimensional, point value, to a vector based characterization of each target. Possible additional considerations might include the military value of a nearby facility or the value associated with an additional, interdependent infrastructure such as communication, transportation, gas pipeline, etc.

6.4.4 Local versus Global Search

The interplay between local and global search is reflected in the bounds placed on the maximum velocity (v_{max}) and the momentum term. By extending the limits on the sigmoid transformation curve the search for the best target sites becomes more global and vice versa. In addition, the rate at which the velocity changes between iterations

Target	Value	Target	Value	Target	Value	Target	Value	Target	Value
1	22	6	48	11	16	16	8	21	43
2	25	7	25	12	36	17	22	22	1
3	20	8	48	13	17	18	39	23	30
4	18	9	39	14	37	19	11	24	13
5	20	10	4	15	14	20	18	25	41

Table 3: Target Values for Momentum/Velocity Comparison

effectively reflects the increase/decrease in confidence that the 'searchers' have after each iteration. By reducing (increasing) the confidence after each iteration, the search is made slower (faster) and the chance of being trapped in a local minimum or maximum is reduced.

A special test case was constructed to test the ability of the algorithm to distinguish between high value and low value targets, and to pick the very best/optimum targets from amongst a group of high value targets (see Table 3).

An investigation into the interaction between these variables is summarized in the following figures, with a complete set of figures provided in Appendix A. A matrix of possible momentum and velocity variables is provided for the scenario involving 5 agents searching for the best combination of 4 targets. The 8 targets with the highest disruption values are overlaid on the matrix of results. The final velocity values for each of the 25 potential targets are presented for all nine separate combinations.

Two results summaries are provided, with the first depicting the results after 100 iterations and the second depicting the results after doubling the number of agents to 10. The final summary depicts 5 agents after 200 iterations. This last summary depicts the results after 5x200=1000 simulations which compares in computation effort to the 10x100=1000 simulations in the second summary.

In general, it can be seen that as the search is broadened, $v_{max} \Rightarrow 6$, and the specific optimum targets begin to be identified sooner. This is evident through the increased number of higher *attack probabilities* associated with the true optimum targets. This suggests the possible approach of doing some initial screening searches to identify a smaller set of targets over which to conduct the search. Also, as the momentum is increased, the best combination of targets is more 'crisply' identified.

As expected, comparing Figure 10 and 12, as the number of simulations increases (100 to 200 in this case) the true set of optimum targets emerges. However, it is interesting to compare Figure 11 and 12 and observe that, while the number of simulations is identical (i.e. 1000), using a terrorist cell size of 5 rather than 10 identifies an 'adequate' set of sub-optimal points sooner. This is a rather counterintuitive and interesting result that will be the basis for future research specifically in particle swarm optimization.

Based on these preliminary investigations, it was decided to focus the search on more complex problems using a maximum velocity in the neighborhood of 5.0 and a momentum greater than 0.90.

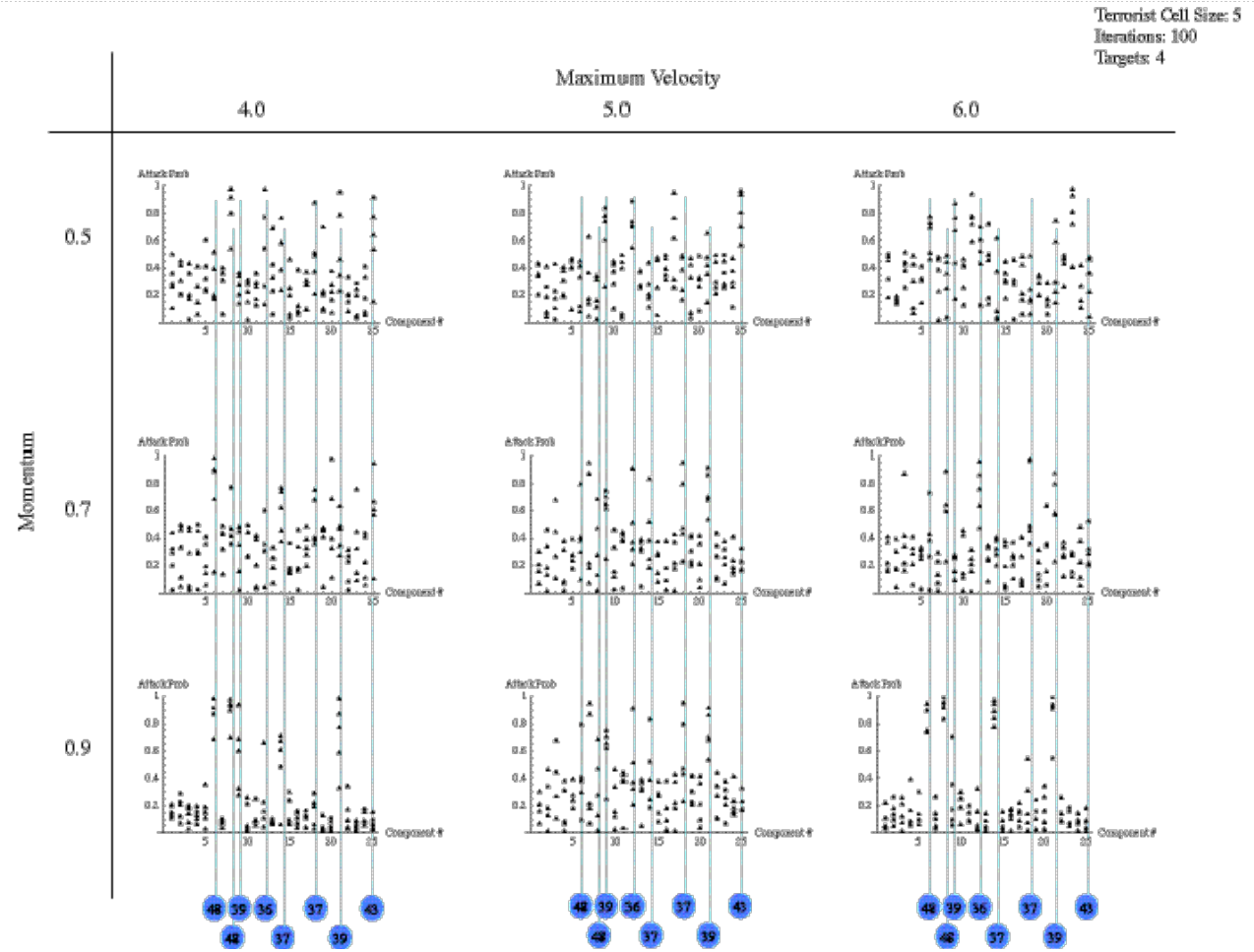


Figure 10: Momentum versus Velocity – 5 agents:4 targets: 100 iterations

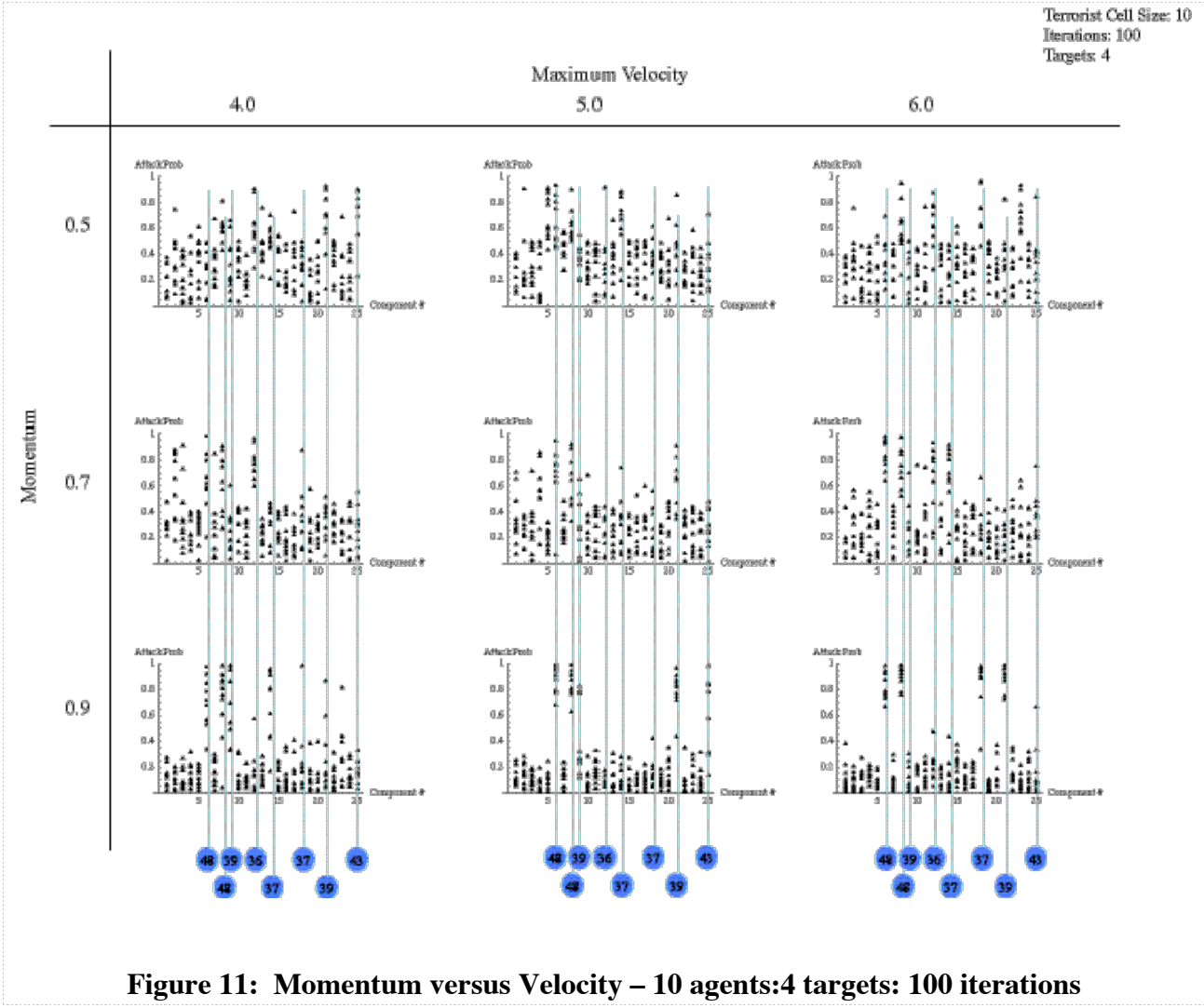


Figure 11: Momentum versus Velocity – 10 agents:4 targets: 100 iterations

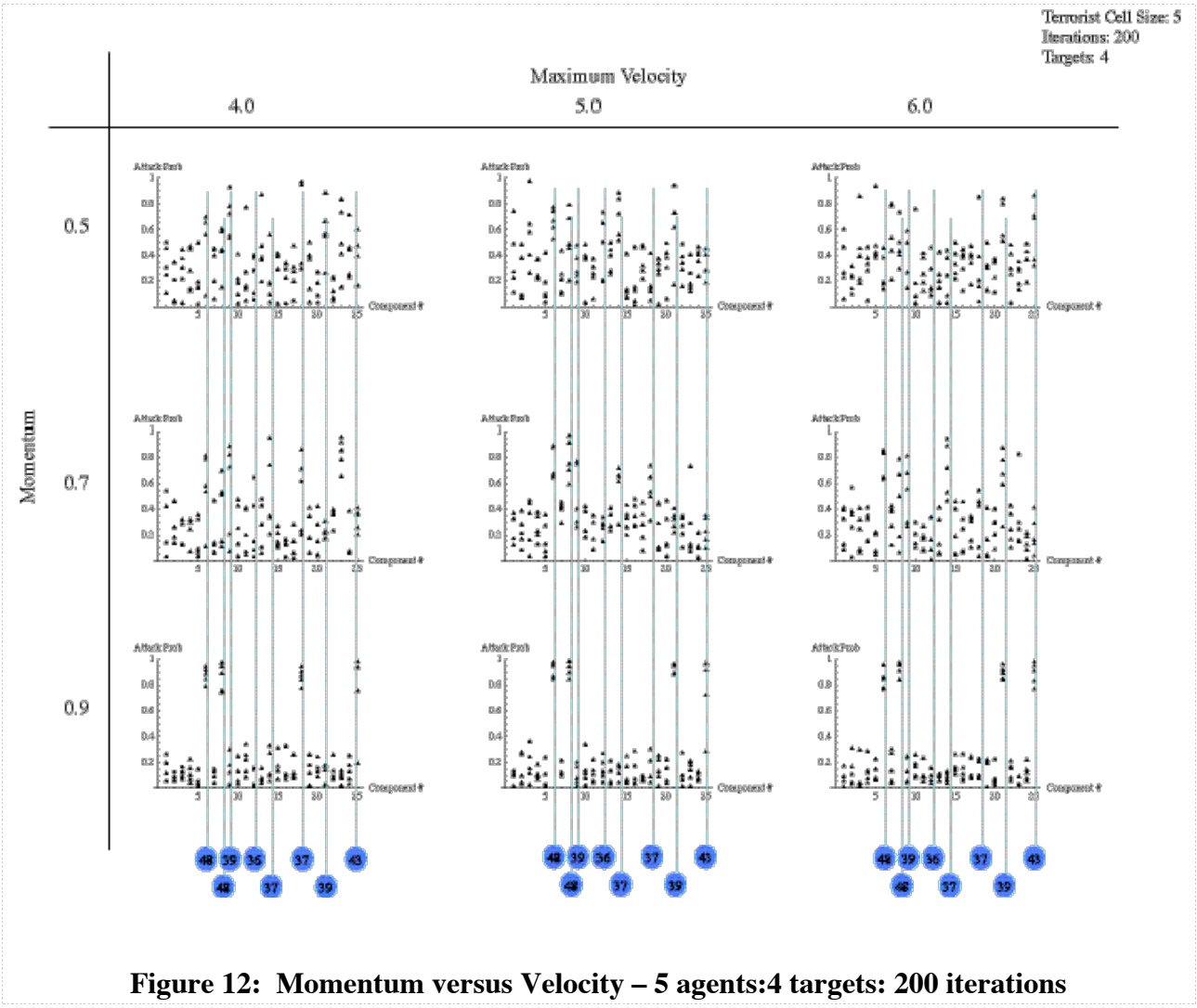


Figure 12: Momentum versus Velocity – 5 agents:4 targets: 200 iterations

7.0 Implementation

7.1 Analysis Approach

In this investigation, the first approach involved interfacing the Buzzard instigator software with a network analysis tool and collecting the changes taking place in network diameter and cluster coefficients as nodes (and edges) were removed from the network. Modeling the bulk power network as an undirected, unweighted graph would permit extremely fast analysis of very large power systems. While this posed an interesting scenario, the current literature suggests that existing network performance measures (e.g. diameter) do not provide acceptable measures for characterizing the impact of disruption on the performance of the bulk power system. (It was felt that investigation of alternative performance measures at some future time may yield better results.)

An alternative approach involved interfacing the Buzzard software directly with an actual power flow simulation program. This would provide the capability to observe (within the constraints of the simulation model) the impact of disrupting the power system. However, this presented some difficulties. Given the vast number of contingency scenarios to be investigated, the computational burden would still be substantial.

As an approximation, it was decided to make a number of simplifying assumptions. First, since a complete characterization of network reliability measure is not needed, only deterministic performance measures need to be considered. Second, after a network disruption, only the very immediate impact on the power flow in the grid would be characterized and collected for each scenario.

The specific performance measure and the two different power flow analysis packages investigated are described in the sections below.

7.2 Performance Measures

Since many performance assessment results must be compared during contingency analysis, there is a need to reduce the voluminous output of a power grid simulation to a manageable number of performance measures. All formal contingency assessments involve comparing a single index, or multiple indices, against some simple numeric standard. Also relevant to contingency analysis is the identification of failure criteria. These failure criteria include capacity deficiency, line overload, system separation with load loss, bus isolation with load loss, voltage collapse, MVAR limit violations, and non-convergent situations (which surrogate network instabilities). When a contingency fails, either an index is greater than some critical value or is outside of some believed-stable region of index values, or some failure criterion is met. These performance indices can themselves be the direct product of a contingency analysis model, without any intermediate derivation of more precise information such as power flow calculations, at the expense of precision and accuracy. Indices that avoid full power flow calculations to determine post-contingency voltage levels at each bus have shown promise in reducing computation time while still supporting ranking and screening procedures [23, 113, 114, 115, 116].

Such an approach was chosen here; the measure chosen, line voltage and current overrating, is commonly used in contingency analysis of bulk power systems. Line overrating is expressed as a percentage of the allowable load, either voltage or current, that is placed on the system. Under normal operation, a line rating of 100% is typical. It was felt that the change in line overrating immediately subsequent to a disruption would provide at least a qualitative measure of the severity of the disruption.

To compare contingencies, a single performance measure or cost function was developed: the sum of all line overratings which exceed a particular criteria. Critical overratings vary slightly from area to area (105%-110%) but for the purposes of this study a single criterion is used. Unless specifically noted otherwise, a limit of 110% is used as the critical level for all the cases discussed.

To characterize the performance of a network before and after disruption, two open source power flow packages were employed. The first was developed by New Mexico State University under contract to Sandia National Laboratories. The second is a product with a long history that has been developed by the Bonneville Power Association (BPA).

7.3 Power Flow Software

To evaluate the impact of computer generated contingency, an open source power flow computer package is needed.

7.2.1 PFLOW

When this project was first started, no open source power flow analysis software was

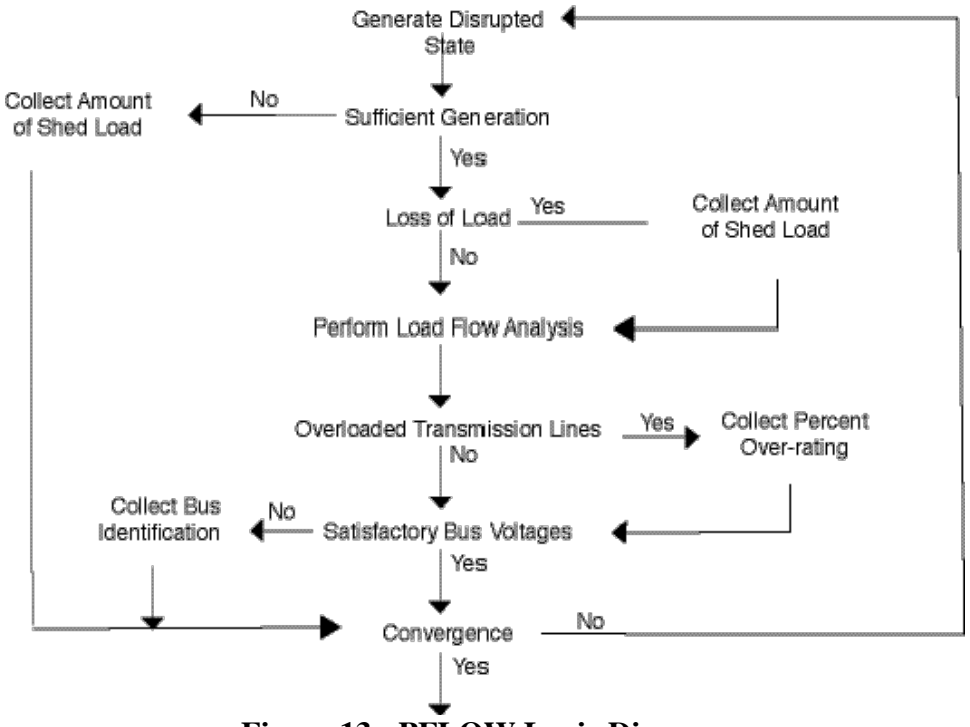


Figure 13: PFLOW Logic Diagram

available, and a cooperative effort was initiated with New Mexico State University to develop a simple package of code. The PFLOW program was developed by Dr. Satish Ranade (Department of Electrical Engineering, New Mexico State University) under contract to Sandia National Laboratories. The program consists of a library of routines to perform power flow, short circuit, stability, equivalencing and harmonic propagation studies for three-phase power systems. The system is assumed to be balanced and sequence networks are used to model unbalanced faults and harmonics.

For power flow analyses, the program includes various power flow solution techniques including the Stott fast-decoupled load flow. Sparse matrix/vector techniques are used throughout. The sequence-network approach is used to perform fault studies, and transient stability studies utilize a trapezoidal rule solution technique and classical generator models.

The PFLOW program has been utilized for a number of power grid reliability projects at Sandia National Laboratories. Figure 14 presents the interface for an analysis approach initially investigated under this research. The system depicted is a simple IEEE 5 bus Reliability Test System. The objective of the analysis was to characterize the probability of shedding of load at various points within the network. The blue ellipses are 'roll-overs' where the user could obtain information about the amount of load shed at a bus. Inputs included traditional contingency information (e.g. random failure of network elements) as well as uncertainties in consumer usage characteristics in the form of probability

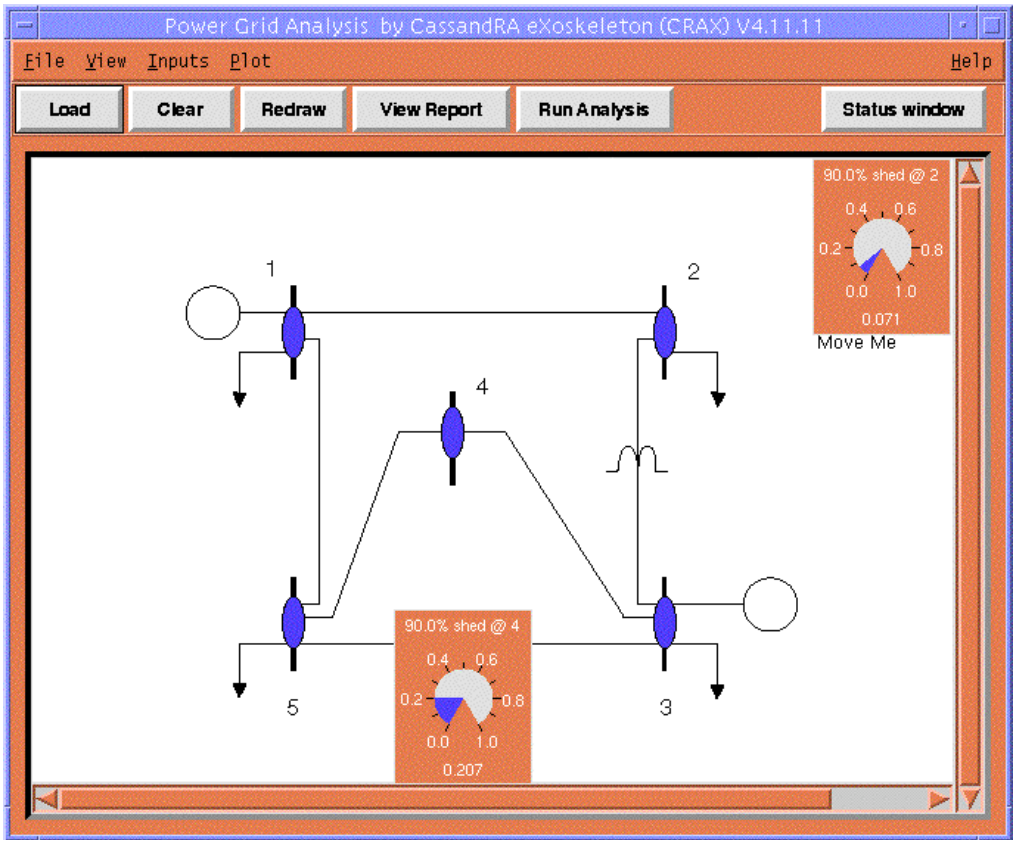


Figure 14: PFLOW/Cassandra Analysis User Interface

distributions for the load at each bus.

The analysis approach holds a great deal of promise to support a risk-based level of generation reserves in response to, for example, variations in summer temperatures that place unexpected demands on the power system. However, in this instance, this approach resulted in interesting results but did not provide immediate information about the importance of specific nodes, and its suggested use is as a post-contingency processing analysis after critical nodes are identified.

The program is limited by the size of the network (e.g. number of nodes) that can be modeled (~ 1000 nodes) and accurately analyzed and the ability to model DC ties. The software is extremely easy to use for small- or moderate-sized bulk power systems, but is unsuitable for the larger networks that are the eventual objective of this research.

The difficulty with extending the PFLOW software became evident late in the project and it was decided to investigate alternatives. By this time, BPA had developed and validated a large power flow program and made it available for public use.

7.2.2 BPA/IPF

Over the past 20 years, BPA has been actively involved with the development of power system analysis software. In 1991, BPA, in partnership with WECC and the Electric Power Research Institute (EPRI), began development of an enhanced power flow package referred to as the Interactive Power Flow (IPF) program. This program is available in either a 'batch' version or a version that includes a graphical user interface (GUI).

IPF can be used by engineers for the design and planning of large power networks and provides information on:

- Bus voltage distribution.
- Line real and reactive power flows.
- Line overloads.
- System reactive requirements.
- Area interchange control.
- Transformer tap settings.
- Remote-bus voltage controls.
- Effects of load shedding, generator dropping, line outages, etc.

The program uses advanced techniques of large-system analysis (including the Newton-Raphson method of solving algebraic equations) coupled with sparse-matrix computation techniques.

7.3 Buzzard

Buzzard is a software program that acts as an instigator to computer models of large complex systems by introducing a failure in a set of components, e.g. a contingency. The algorithm embedded within Buzzard is independent of the particular system model or infrastructure, but the most recent application has been for Buzzard to act as a cell of terrorists with a goal to cause maximum damage to bulk power networks.

Buzzard uses the previously discussed AI-based swarm theory algorithm to develop a set

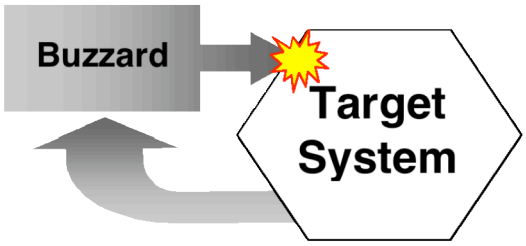


Figure 15: Target System/Buzzard Interaction

of scenarios for disrupting the system. These scenarios are introduced into the system and incite a reaction from the system. The reactions that result are observed by Buzzard and a new set of scenarios are constructed to stimulate the target system. These new scenarios are constructed in an evolutionary fashion such that Buzzard seeks new and more effective provocations to disrupt the system.

The complexity of the scenarios is predetermined by the user along with the particular measures that characterize the impact of the scenarios on the system.

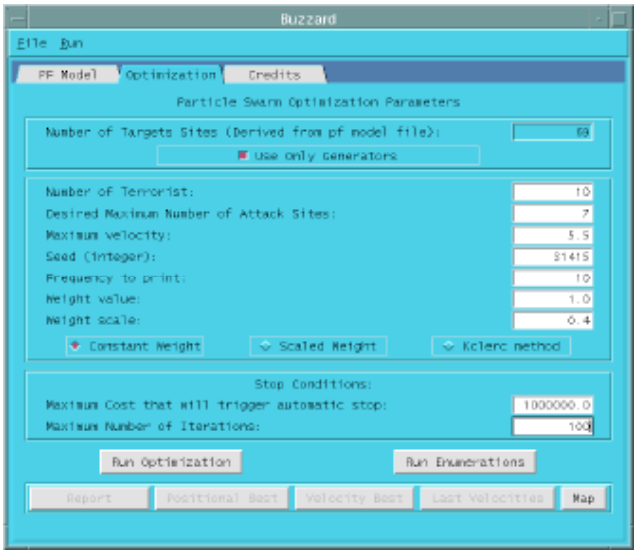


Figure 16: Buzzard Swarm Interface

The evolutionary strategies within Buzzard differ significantly from approaches that commonly apply genetic-based algorithms as a basis for their search algorithms. Contrary to the algorithms in Darwinism-based paradigms, individuals are not replaced by better performing individuals. Rather, the individuals within Buzzard adapt to the environment by gathering information and processing that information as a group. In this approach it

is not the individual who changes, but rather the knowledge of the individual that changes each time a new scenario is generated.

In addition, unlike genetic-based algorithms, the algorithms within Buzzard are less susceptible to being trapped within local minima. Buzzard algorithms are all coded in C/C++ and are scalable to the particular size of system being targeted. The GUI for Buzzard is summarized in Appendix B. Buzzard GUI windows for the swarm optimization and bulk power map output window are presented in Figures 16 and 17.

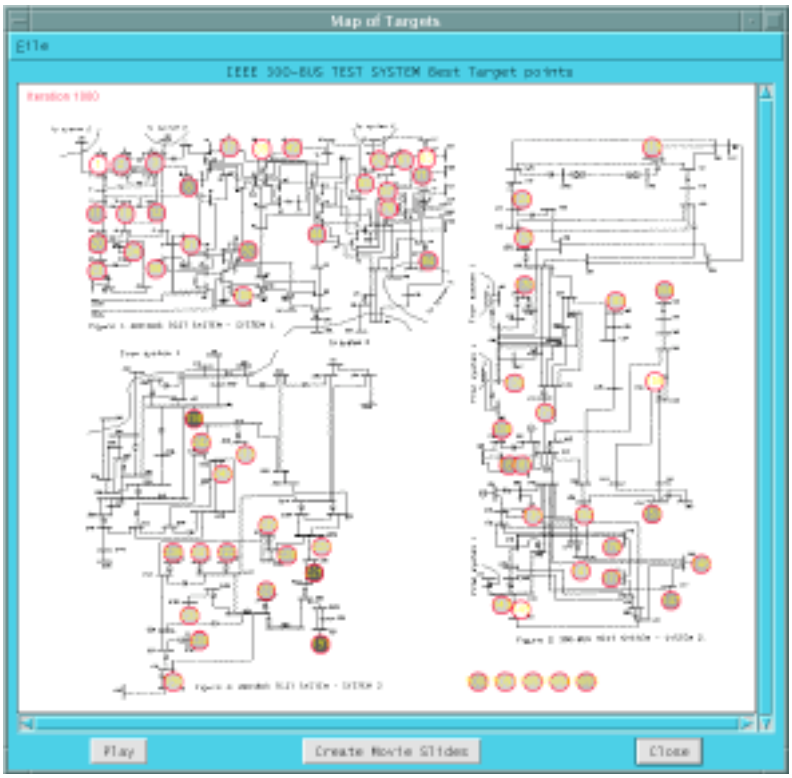


Figure 17: Buzzard Bulk Power Output Map

7.3.1 Buzzard Simulation Structure

Figure 18 depicts the steps in the simulation to assess the performance index:

1 Buzzard attacks physical and SCADA system.

2 Buzzard initiates SCADA.

3 Using available communication equipment, the SCADA queries physical model.

4 Physical model queries network state.

5 SCADA model reconfigures network in response to degraded network.

6 SCADA model passes control to physical model.

7 Physical model queries physical state and characterizes power system performance and then feeds performance back to Buzzard.

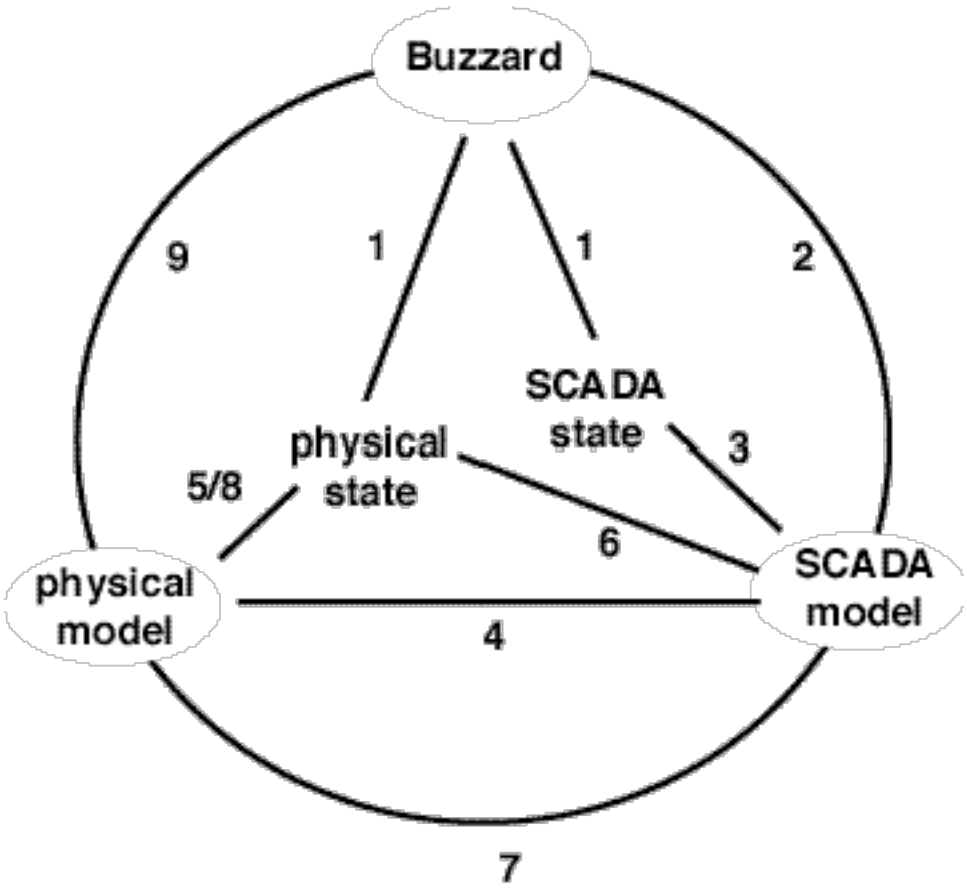


Figure 18: Buzzard/SCADA/Power Flow Information Exchange

Buzzard then determines the 'value' of the attack scenario and suggests a new approach to attack the network.

For the analyses that follow, no SCADA equipment was included in the analysis, since the SCADA model was still in development at the time this report was prepared. However, all software 'hooks' were developed so that when the model does become available it will be rather straightforward to integrate.

8.0 Test Cases

The simplest test case used during the course of this research was the IEEE 5 bus Reliability Test System (RTS).

Figure 19 depicts the very simple power network consisting of only 5 buses, 2 generators, 4 loads and a single transformer. There are 8 different elements. This network was used only for the initial investigations involving the introduction of stochastic demand into a traditional bulk power system adequacy analysis. This is the system used in the PFLOW/Cassandra analysis discussed in Chapter 7.

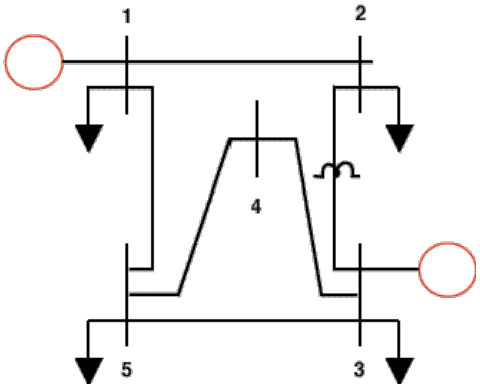


Figure 19: Simple 5 Bus Test System

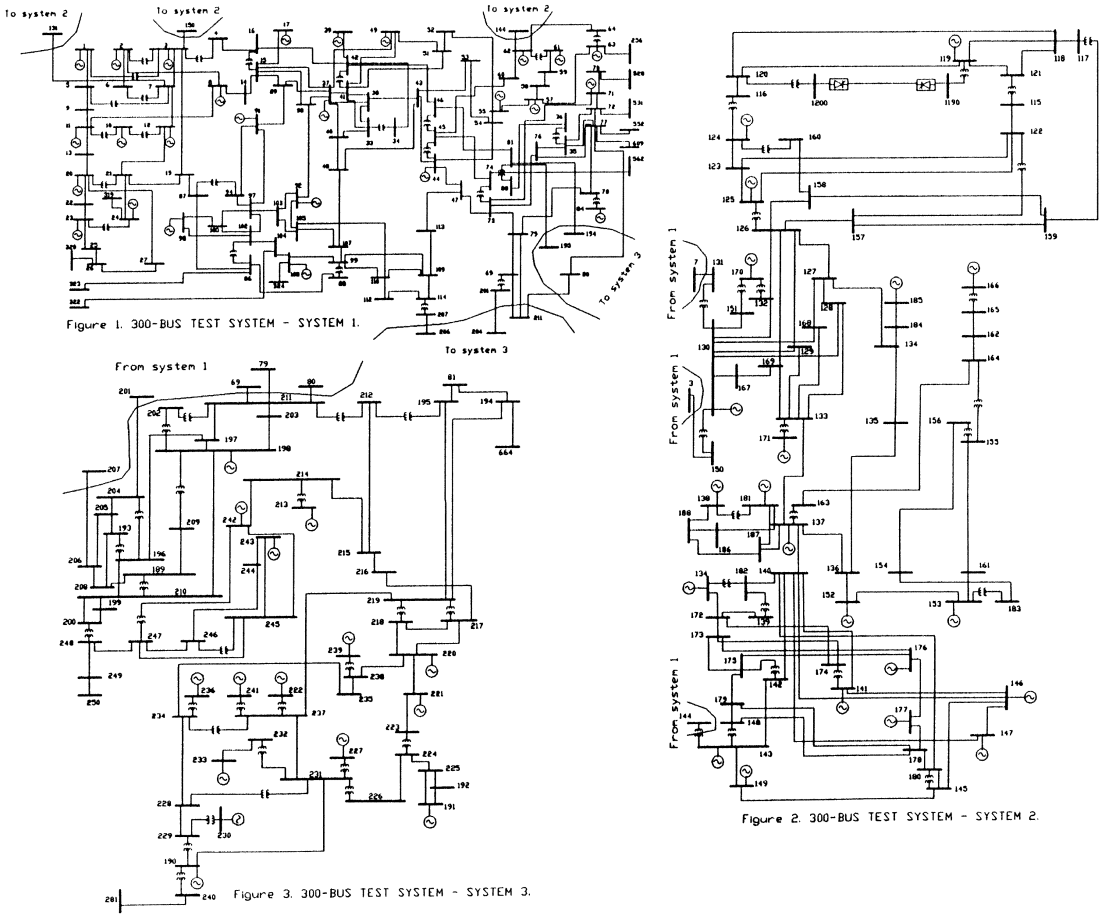


Figure 20: IEEE 300 Bus Reliability Test System

It was eventually decided that the system was too simple for the more advanced methods that were to be investigated, and the IEEE 300 bus test system was chosen as the basis for further research.

The IEEE 300 bus test case was initially developed by the IEEE Test Systems Task Force in 1993 based on data from a northeast power pool. The particular data set used in this analysis is available from the University of Washington Power System Test Case Archive. The site provides World Wide Web access to power system data (test cases) and is maintained by Richard D. Christie, an Associate Professor at the University of Washington, Seattle, Washington, USA (christie@ee.washington.edu). The system consists of three connected regions as depicted in Figure 20 with 69 generators and 298 busses, transformers, etc. available for disruption.

For the initial investigation it was decided that a subset of the IEEE 300 RTS would be appropriate. A reduced test system was developed, focusing only on the 69 generators in the network. This network is depicted in Figure 21, with the generators identified and numbered. (Generators 65-69 are included in the computer model as reserve generators.)

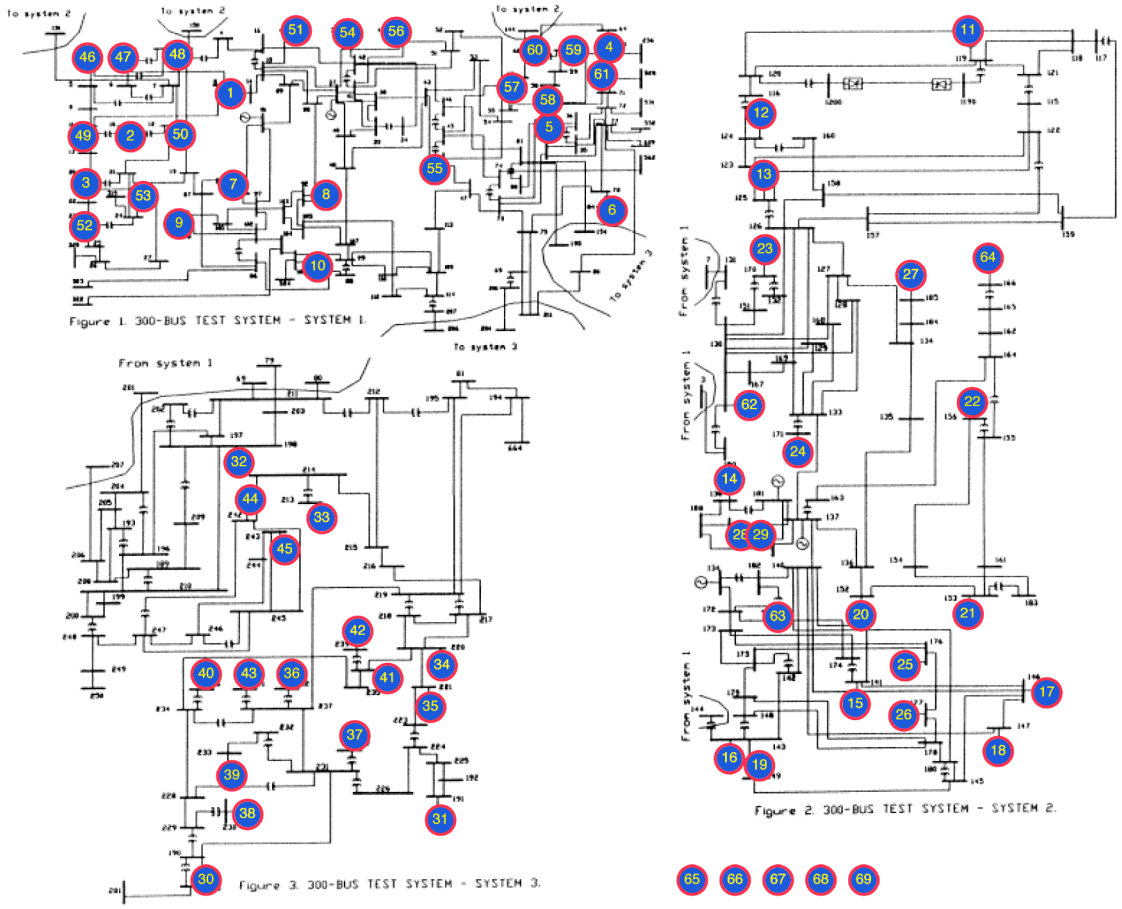


Figure 21: 69 Generator Reliability Test System

9.0 Results

9.1 Enumeration: Exact Solution

The number of possible target combinations is incredibly large even when limiting the analysis to the 69 generators. When limiting the allowable number of targets to 2 there are 2,346 possible contingencies, while for 3 targets the possible target scenarios explodes to 52,394 and for 9 there are 56,672,074,888. Validation and verification of the algorithms is obviously very difficult and verges on being computationally impossible.

For this initial research, the focus was on identifying the best combination of modeling parameters to identify the best 2 or 3 targets since it was possible to actually enumerate all possible target combinations of these sizes. Table 4 presents the results for 2 possible attack sites from a set of 69 possible targets. The cost (damage) associated with each target combination is provided as well as the names and bus reference number (in parentheses) of each target. Table 5 summarizes the results for scenarios involving 3 attack sites.

Cost	Target Set: 2 node scenario	
88106	31 (191)	10 (108)
8809	31 (191)	61 (7071)
87471	31 (191)	51 (7017)
87306	31 (191)	45 (243)
87086	31 (191)	8 (92)
86961	31 (191)	11 (119)
86724	31 (191)	30 (190)
86620	31 (191)	35 (221)

Table 4. Optimal 2 Target Sets : Truth

These results are summarized in Figures 22 and 23 respectively. Note: the green nodes belong to one or more optimal target sets.

It is interesting to note that there are significant differences between the general locations of the critical nodes for the two different cases. With the exception of Generator 31 there is no overlap between the top 7 optimal target sets between the optimal target sets for each type of scenario. The differences between the distribution of optimal attack sites for each type of scenario across the entire network is clearly seen in Figures 22 and 23. Targets for the 2 nodes attack scenarios are typically distributed across two subnetworks, while the targets for the 3 node scenarios are focused in a single subnetwork.

Cost	Target Set: 3 node scenario		
90342	31 (191)	40 (236)	33 (213)
90151	31 (191)	40 (236)	42 (239)
90105	31 (191)	40 (236)	41 (238)
90104	31 (191)	40 (236)	29 (187)
90095	31 (191)	32 (198)	42 (239)
90082	31 (191)	39 (233)	42 (239)
90050	31 (191)	40 (236)	28 (186)
90030	31 (191)	32 (198)	43 (241)

Table 5. Optimal 3 Target Sets: Truth

It is also important to note that the set of seven solutions summarized in the above tables reflect (effectively) multiple, optimal solutions, since the differences between the costs are negligible.

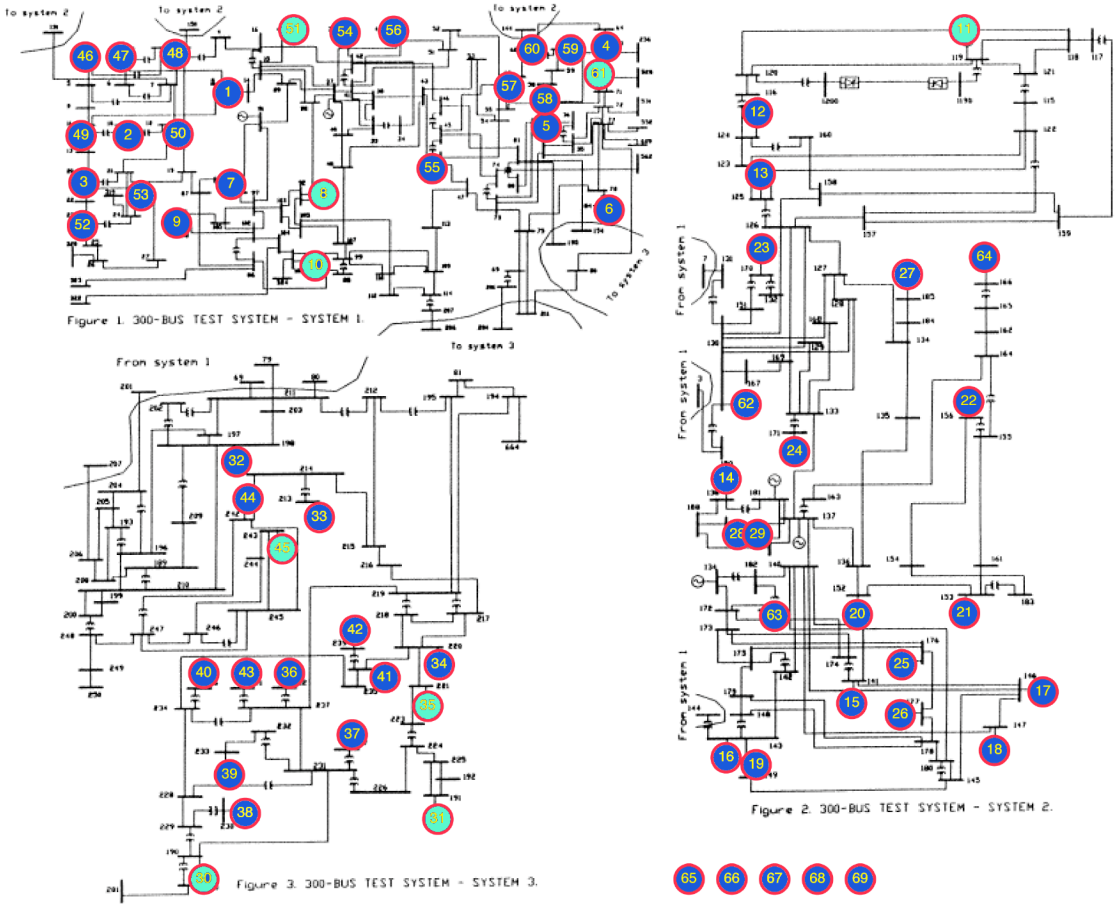


Figure 22: Distribution of Target Generators (2 Target Scenarios)

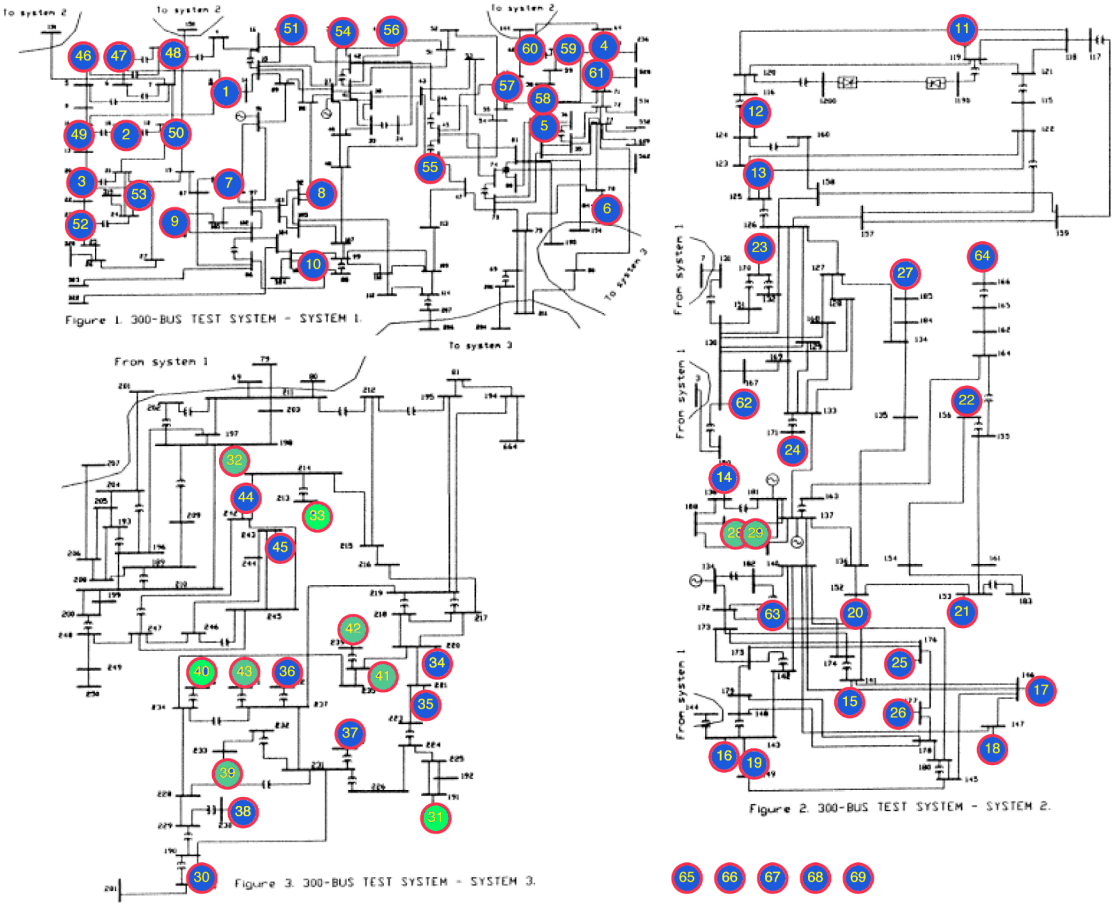


Figure 23: Distribution of Target Generators (3 Target Scenarios)

9.2 Swarm Algorithm Implementation

The Buzzard software implementing the swarm search algorithm was integrated with the NMSU power flow code and a number of bulk power networks were analyzed. The following summarizes the results for the IEEE 300 RTS that has been the focus of the discussion. The emphasis in this report is on the testing and validation of the Buzzard implementation and not on the identification of vulnerable points in an actual bulk power system. Once validation is complete, application to a larger, more complex network is rather straightforward.

As noted previously, the testing and validation was limited to identification of the best targets from the set of 69 generators within the IEEE 300 RTS. Two scenarios were investigated which involved identifying the best set of 2 or 3 targets. A variety of terrorist cell sizes (number of agents) were investigated along with a variety of momentum factors and maximum velocities (v_{max}).

In retrospect, the choice of the standard IEEE 300 RTS was unfortunate. There are a large percentage of network elements that can have very similar operational impact on the performance of the system. In addition, these sets differ in their value (cost) by only roughly 5%. This made validation a bit more challenging than would be expected from an actual bulk power system.

Table 6 presents the summaries for two investigations into optimum target sets of size 2 and 3 for cell sizes 5, 7 and 9. Momentum factors were set to 1.0 and v_{max} = 5.0 for all scenarios. It is clear that the algorithm quickly identifies a set of critical nodes, but it can take considerable additional computational effort to identify the true optimum target set. For example, for a target set size of 2 and a cell size of 9, the algorithm quickly (150 iterations) finds a target set that is within 0.26% of the optimum, but requires another 4000 iterations to find the true 'best' pair of targets.

Target	Cell Size	Penalty Cost	Momentum	Vmax	Iterations	Cost	Target Set	First Top 7	Alt Cost
2	5	10000	1.0	5	2975	88106	31,45	150	86620
	7	10000	1.0	5	5350	88106	31,10	225	87085
	9	10000	1.0	5	4150	88106	31,10	150	87306

Target	Cell Size	Penalty Cost	Momentum	Vmax	Iterations	Cost	Target Set	First Top 7	Alt Cost
3	5	10000	1.0	5	175	90103	31,29,40	175	90103
	7	10000	1.0	5	125	90095	31,32,42	125	90095
	9	10000	1.0	5	3525	90342	31,33,40	450	90105

Table 6. Summary of Investigations for Target Sets of Size 2 or 3

Table 7 presents the summaries for scenarios involving a cell size of 7 and a target set size of 3 for various combinations of momentums and v_{max} . The number of iterations was artificially capped at 150; no exhaustive attempt at identification of the final optimum set was conducted.

From Figure 24 it is clear that by reducing the momentum factor, the convergence to the optimum target set is slower. The number of potential targets with high probability of

selection as a target is still rather large for a momentum of 0.90 and decreases rapidly as the momentum factor is reduced to 0.95 and then finally to 1.0. *This can be useful if, rather than attempting to identify a specific set of X targets, it is simply desired to identify a larger set of important targets perhaps with the intent of identifying vulnerable regions within a bulk power network.*

Alternatively, the impact of v_{max} on the identification of the optimal target set is less distinct. For a specific momentum, in this case 1.0, the cost function quickly focuses on the selection of 3 targets. Larger values of v_{max} allow the search for the optimum to extend over a broader region of support and the algorithm is less likely to be 'stuck' in a local minimum.

In reviewing all these results, it is important to recognize that the swarm search algorithm is a stochastic search algorithm – variations in the initial seed will potentially result in small variations in the target set identified. As noted previously, it is important to conduct a few simulations with different initial seeds to better understand the network being analyzed.

Target	Cell Size	Penalty Cost	Momentum	Vmax	Iterations	Cost	Target Set
3	7	10000	1.00	5.0	150	90151	31,40,42
	7	10000	0.95	5.0	150	66442	No convergence
	7	10000	0.90	5.0	150	-8214	No convergence

Target	Cell Size	Penalty Cost	Momentum	Vmax	Iterations	Cost	Target Set
3	7	10000	1.0	5.0	150	90151	31,40,42
	7	10000	1.0	5.5	150	89095	31,35,63
	7	10000	1.0	6.0	150	88359	9,31,51

Table 7: Summary of Investigations for Various Momentum, Vmax Values

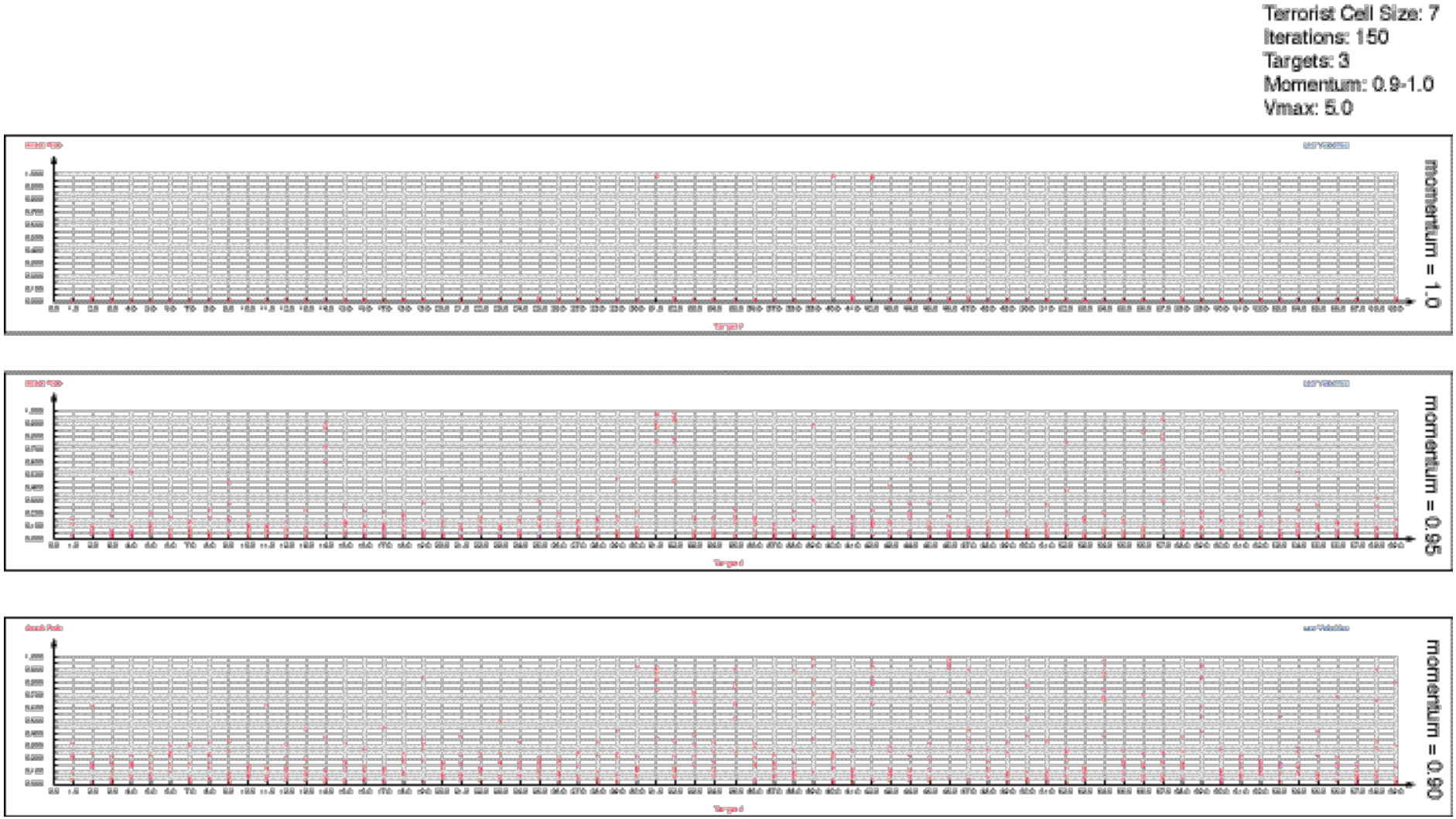


Figure 24 Final Velocities for Cell Size 7, Vmax=5.0, Momentum=[0.9-1.0]

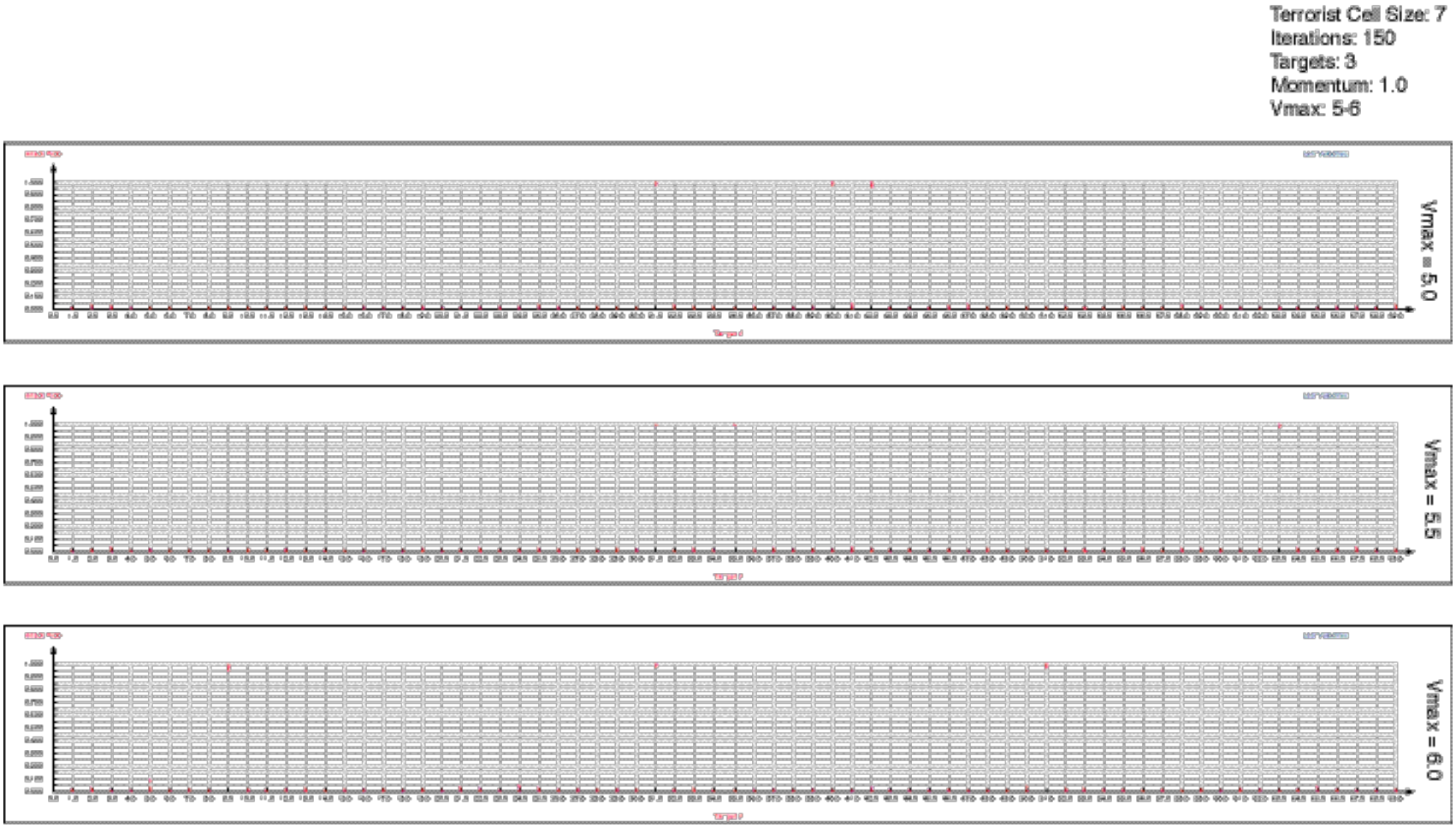


Figure 25: Final Velocities for Cell Size 7, Vmax=[5.0-6.0], Momentum=1.0

10.0 Conclusions and Recommendations

It is clear that the Buzzard software coupled with a traditional power flow analysis program can be used to identify critical elements within large complex bulk power systems. The algorithms are consistent with traditional methods that identify critical single point contingencies in the sense that the new approach can also be used to characterize single point contingencies. For small numbers of potential attack sites (e.g. 2-3) on relatively small systems (69 nodes) it was possible to enumerate all possible contingencies and in every case the nodes identified through enumeration corresponded to the nodes identified using the Buzzard algorithm.

10.1 Observations

The software very quickly identifies one of the multiple 'best' solutions. As mentioned previously, for the given cost function, there are a number of best solutions that are very close in value. The algorithm typically finds a solution that is within 0.3% of the value of the true optimum, but may require 5000 iterations to find the final best target combination.

The existence of multiple, sub-optimal solutions with very similar total target values poses a bit of a dilemma: it is important to be aware of similar 'optimal' solutions, but it clouds identification of the 'best'. It is suggested that a small number of additional searches be conducted with various initial seed values before identifying a specific set of targets. In addition, the velocity vector provides considerable insight into the existence of these potential members of the optimal set. High residual velocities at the completion of the simulation are key indicators of potential optimal set membership.

Two key considerations that need to be understood and possibly investigated in a more formal fashion in future efforts: sensitivity to v_{max} and the penalty associated with exceeding the allowable number of target locations. The choice of v_{max} impacts the search algorithm by constraining the search to be either more locally focused or allowing the search to extend to a more global solution space. Typically, $3 < v_{\max} < 6$, with smaller values being associated with local search and larger values allowing the search to broaden. Penalties over the range of 1000 to 10,000 were used to force the number of selected targets to be approximately the user specified values. High penalties coupled with low values of v_{max} resulted in lengthy simulations until convergence.

10.2 Future efforts

Future efforts should be directed at developing a better cost function with emphasis on perhaps a correct penalty value for exceeding the maximum number of targets. In addition, a better stopping rule is required to allow slightly sub-optimal solutions to be identified earlier.

The swarm algorithms are not limited by the particular failure indicators chosen in this research (e.g. line overrating). Other indicators such as the amount of load shed could easily have been used. Further, specific targets may have unique value due to the economic or military infrastructures that are lost through disruption of particular nodes; it

would have been rather straightforward to include the value of particular targets in the cost function for the optimization. It is also possible to extend the value function for each node to a multi-dimensional characterization to include not only, for example, line rating, but simultaneously consider shed load.

For computational reasons, higher order attack scenarios coupled with high dimensional systems (high number of potential nodes for attack) could not be investigated. However, the algorithms are scalable and there is every reason to expect that they would be equally effective on more complex systems.

Non-linear (i.e. *ac*) power flow analysis was used in all the test cases. It is strongly suggested that future investigation use linear analysis (i.e. *dc*) for power grid analysis to speed up the processing time. The original research objective for using a nonlinear power flow analysis was to assist in identifying contingencies that would lead to network instabilities. This would have provided a great deal more information about the impact of disrupting particular targets, but time and resources did not permit extending the analysis to this level of detail.

In summary, the approaches suggested and tested within the confines of this research have tremendous potential, but before final implementation, significant validation and verification simulations must be performed.

Acknowledgements

This research was conducted with support from the Laboratory Directed Research and Development program at Sandia National Laboratories. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000. The author wishes to particularly thank Lee Eubanks, GRAM, Inc. who did the majority of the programming associated with the above analyses.

Reference List

[1] North American Electric Reliability Council. *Preparing the Electic Power Systems of North America for Transition to the Year 2000*. ftp://ftp.nerc.com/pub/sys/all_updl/ docs/Y2k/secondfinalreporttodoe.pdf, February 14, 1999.]

[2] Schilling, M., Leite De Silva, A., Billinton, R., El-Kady, M.,"Bibliography on Power System Probabilistic Analysis (1962-1988)", IEEE Transactions on Power Systems, Vol.5, No. 1, February 1990, pp. 41-49

[3] Allan, R. Billinton, R., Breipohl, A., Grigg, C.,"Bibliography on the Application of Probability Methods in Power System Relibility Evaluation 1967-1991", IEEE Transactions on Power Systems, Vol. 9, No. 1, February 1994, pp. 41-49

[4] Pereira, m., Balu, N.,"Composite Generation/Transmission Reliability Evaluation", Proc. IEEE, Vol. 80, No. 4, April 1992, pp.470-49

[5] Allen, Ron and Roy Billinton, Power-system reliability in perspective, Electronics and Power, March 1984, pp. 231-236.

[6] EPRI, Composite-System Reliability Evaluation: Phase 1 – Scoping Study, EPRI EL-5290, Final Report, December 1987.

[7] Allan, Ron, R. Billton, et al., Reliability Assessment of Composite Generation and Transmission Systems, IEEE Power Engineering Society Tutorial, 90EH0311-1-PWR, 1989.

[8] Allan, Ron and Roy Billinton, Probabilistic Assessment of Power Systems, Proceedings of the IEEE, Vol 88, No 2, February 2000, pp 140-162.

[9] Balu, N. et al, Online Power-System Security Analysis, Proceeding of the IEEE, v 80(2), pp 262-280, Feb 1992

[10] Talukdar, S, VC Ramesh, A Multi-Agent Technique for Contingency Constrained Optimal Power Flows, IEEE Transactions on Power Systems, Vol 9, No 2, May 1994, pp 855-861.

[11] Van Cutsem, Thierry, Voltage Instability: Phenomena, Countermeasures, and Analysis Methods, Proceedings of the IEEE, Vol 88, No 2, February 2000, pp 208-227.

[12] Chang, Chung-Liang and Yuan-Yih Hsu, Deterministic and Probabilistic Contingency Selection, Journal of the Chinese Institute of Engineers, Vol 12, No 6, pp 771-780, 1989.

[13] Lo KL, LJ Peng, et al., An Extended Ward Equivalent Approach for Power System ecurity Assessment, Electric Power Systems Research, Vol 42, 1997 pp 181-188.

[14] Maghraby, HM, AS Farag and AN Cheema, Reliability Equivalents for AC Adequacy Evaluation of Large Power Systems, Electric Machines and Power Systems, Vol 26, 1998, pp 507-527.

[15] Snyder WL, S Vemuri, et al, External Network Modeling – Recent Practical Experience, IEEE Transactions on Power Systems, Vol 9, No 1, Feb 1994, pp 216-228

[16] Fu Y. and TS Chung, A Hybrid Artificial Neural Network (ANN) and Ward Equivalent Approach For On-Line Power System Voltage Security Assessment, Electric Power Systems Research, Vol 53, 2000, pp 165-171.

[17] Mori H, H Tenaka, J Kanno, A Preconditioned Fast Decoupled Power Flow Method for Contingency Screening, IEEE Transactions on Power Systems, Vol 11, No 1, Feb 1996, pp 357-363.

[18] Mohamed AA, H Shaaban, K Kahla, "A fast and accurate technique for circuit contingency evaluation", Electric Power Systems Research, v 45(3), pp 181-189, June 1998.

[19] Harsan, H., N. Hadjsaid, P Pruvot, Cyclic Security Analysis for Security Constrained Optimal Power Flow, IEEE Transactions on Power Systems, Vol 12, No 2, May 1997, pp 948-953.

[20] Wehenkel, L., Contingency Severity Assessment for Voltage Security Using Non-Parametric Regression Techniques, IEEE Transactions on Power Systems, Vol 11, No 1, Feb 1996, pp 101-111.

[21] Sinha, AK, Power-System Security Assessment using Pattern-Recognition and Fuzzy Estimation, International Journal of Electrical Power and Energy Systems, Vol 17, No 1, pp 11-19.

[22] TF Halpin, Fischl R and Fink R, Analysis of Automatic Contingency Selection Algorithms, IEEE Transactions on Power Apparatus and Systems, Vol, 103, No 5, pp 938-945, 1984.

[23] Nahman, J. and I Skokjlev, Fuzzy Logic and Probability-Based Real-Time Contingency Ranking, Electrical Power and Energy Systems, Vol 22, 2000, pp 223-229.

[24] Matos, MA, ND Matziargyriou, JA Pecas Lopes, Multicontingency Steady State Security Evaluation Using Fuzzy Clustering Techniques, IEEE Transactions on Power Systems, Vl 15, No 1, Feb 2000, pp 177-183.

[25] Hsu YY, and HCD Kuo, Fuzzy set based contingency ranking, IEEE Transactions on Power Systems, Vol 7(3), pp 1189-1193, 1992.

[26] Nims JW, AA El-Keib and RE Smith, Contingency Ranking For Voltage Stability Using a Genetic Algorithm, Electric Power Systems Research, Vol 43, 1997, pg 69-76.

[27] Kim, JO, SW Nam, SK Park, C Singh, Dispersed Generation Planning Using Improved Hereford Ranch Algorithm, Electrical Power Systems Research, Vol 47, 1998, pp 47-55.

[28] Lai, LL, New Approach of Using Evolutionary Programming to Reactive Power Planning with Network Contingencies, European Transactions on Electrical Power Engineering, Vol 7, No 3, 1997, pp 211-216.

[29] Hsiao, Y-T, C-C Liu, H-D Chiang, Y-L Chen, A New Approach for Optimal VAR Sources Planning in Large Scale Electrical Power Systems, IEEE Transactions on Power Systems, Vol 8, No 3, August 1993, pp 988-996.

[30] Yoshida, H, K Kawata, et al, A Particle Swarm Optimization for Reactive Power and Voltage Control Considering Voltage Security Assessment, IEEE Transactions on Power Systems, Vol 15, No 4, Nov 2000, pp 1232-1239.

[31] Bonnans, JF, Mathematical Study of Very High Voltage Power Networks III, Computational Optimization and Applications, Vol 16, No 1, 2000, pp 83-110.

[32] Wan, HB, ME Bradley, AO Ekwue and AM Chebbo, Method For Alleviating Voltage Limit Violations Using Combined DC Optimisation and AC Power Flow Technique, IEE Proc.-Gener., Transm. Distrib., Vol 147, No 2, March 2000, pp 99-104.

[33] Dornellas, CRR, AM Olivieras, et al., The Effects of Local and Optimised Power Flow Control Logic in the Reliability Analysis of Bulk Systems, IEEE (?)

[34] Jabr, RA, AH Coonick and BJ Cory, A Homogenous Linear Programming Algorithm for the Security Constrained Economic Dispatch Model, IEEE Transactions on Power Systems, Vol 15, No 3, August 2000, pp 930-936.

[35] Billinton,R and E Khan, A Security Based Approach to Composite Power System Reliability Evaluation, IEEE Transactions on Power Systems, Vol 7, No 1, Feb 1992, pp 65-71.

[36] Granville, S., JCO Mello and ACG Melo, Application of Interior Point Methods to Power Flow Unsolvability, IEEE Transactions on Power Systems, Vol 11, No 2, May 1996, pp 1096-1103.

[37] Wu J-S, A Petri-Net Algorithm for Multiple Contingencies of Distribution System Operations, IEEE Transactions on Power Systems, Vol 13, No 3, Aug 1998, pp 1164-1171.

[38] Tinnium, K, P Rastgoufard, PF Duvoisin, Electric Power Systems Research, Vol 42, 1997, pp 21-25.

[39] Mendes, JC, OR Saavedra, SA Feitosa, A Parallel Complete Method For Real-Time Security Analysis in Power Systems, Electric Power Systems Research, Vol 56, 2000, pp 27-34.

[40] Albuyeh, F., A Bose, B Heath, Reactive Power Considerations in Automatic Contingency Selection, IEEE Transactions on Power Apparatus and Systems, Vol 101, No 1, pp 107-112, 1982.

[41] Chen, Y and A Bose, Direct Ranking for Voltage Contingency Selection, IEEE Transactions on Power Systems, Vol 4, No 4, October 1989, pp 1335-1344.

[42] Brandwajn, V, Y Liu, MG Lauby, “Pre-Screening of Single Contingencies Causing Network Topology Changes”, IEEE Transactions on Power Systems, v. 6(1), pp 30-36, 1991.

[43] Bijwe, PR, J Nanda, KL Puttabuddhi, "Ranking of Line Outages in an AC-DC System Causing Overload and Voltage Problems", IEE Proceedings –C Generation, Transmission and Distribution, v 138(3), pp 207-212, 1991.

[44] Bijwe, PR, DP Kothari and SM Kelapure, An Efficient Approach for Voltage Security Analysis and Enhancement, Electrical Power and Energy Systems, Vol 22, pp 483-486, 2000.

[45] Liu H, A Bose and V. Venkatasubramanian, A Fast Voltage Security Assessment Method Using Adaptive Bounding, IEEE Transactions on Power Systems, Vol 15, no 3, August 2000, 1137-1141.

[46] Jia, Z, and B Jeyasurya, Contingency Ranking for On-Line Voltage Stability Assessment, IEEE Transactions on Power Systems, Vol 15, No 3, August 2000, 1093-1097.

[47] Greene, S., I Dobson, and F. Alvarado, Contingency Ranking for Voltage Collapse via Sensitivities from a Single Nose Curve, IEEE Transactions on Power Systems, Vol 14, No 1, Feb 1999, 232-240.

[48] Gao, B., GK Morison, P. Kundur, Towards the Development of a Systematic Approach for Voltage Stability of Large-Scale Power Systems, IEEE Transactions on Power Systems, Vol. 11, no 3, August 1996, 1314-1324.

[49] Albuyeh, F. , Automated Contingency Selection by Sensitivity Matrices, IEEE Power Engineering Society Winter Meeting, New York, 1980.

[50] Mikolinnas TA and BF Wollenberg, An Advanced Contingency Selection Algorithm, IEEE Transactions on Power Apparatus and Systems, Vol, 100, No 2, pp 608-617, 1981.

[51] Hadjsaid, N., et al, "Fast Contingency Screening for Voltage-Reactive Consideration in Security Analysis", IEEE Transactions on Power Systems, Vol 8(1), pp 144-151, Feb 1993.

[52] Ejebe, GC, BF Wollenberg, Automatic Contingency Selection, IEEE Transactions on Power Apparatus and Equipment, PAS-98, pp 77-109, Jan/Feb 1979.

[53] Irisarri, GD, D Levner, AM Sasson, Automatic Contingency Selection for On-Line Contingency Analysis – Real-Time Tests, IEEE Transactions on Power Apparatus and Equipment, PAS-98, pp 1552-1559, Sept/Oct 1979.

[54] Carpentier, JL, PJ Di Bono, P J Tournebise, Improved Efficient Bounding Method for DC Contingency Analysis Using Reciprocity Properties, IEEE Transactions on Power Systems, Vol 9, No 1, Feb 1994, pp 76-84.

[55] Brandwajn, V., "Efficient Bounding Method for Linear Contingency Analysis", IEEE Transactions on Power Systems, v. 3(1), pp 38-43, 1988.

[56] Castro, CA, A Bose, E Handschin, W Hoffmann, "Comparison of different screening techniques for the contingency selection function", International Journal of Electrical Power and Energy Systems, V 18(7), pp 425-430, Oct 1996.

[57] Galiana, F., Bound estimates of the severity of the outages in power system contingency analysis and ranking, IEEE Transactions on Power Apparatus and Equipment, PAS-103, pp 2612-2622, 1984.

[58] Ejebe, GC, RF Paliza, WF Tinney, An adaptive localization method for real-time security analysis, IEEE Transactions on Power Systems, Vol 7(2), pp 777-783, 1991.

[59] Montagna, M., GP Granelli, "Bounding method based on generalised real power distribution factors:, IEE Proceedings – Generation, Transmission and Distribution, v. 144(3), pp 249-256, May 1997.

[60] Brandwajn V., MG Lauby, "Complete Bounding Method for AC Contingency Screening", IEEE Transactions on Power Systems, v 4(2), pp 724-729, 1989.

[61] TK Parandhama, A Fast Algorithm for Contingency Evaluation of Power Systems, International Journal of Electrical Power and Energy Systems, Vol 12, No 1, pp 61-64, 1990.

[62] La Scala, M., G Lorusso, R Sbrizzia, M Trovato, A Qualitative Approach to Transient Stability Analysis, IEEE Transactions on Power Systems, Vol 11, No 4, Nov 1996, pp 1996-2002.

[63] Srivastava, L, SN Singh and J Sharma, Parallel Self-organising Hierarchical Neural Network-Based Fast Voltage Estimation, IEE Proc.- Gener. Trans. Distrib. Vol 145, No. 1, Jan 1998, pp 98-104.

[64] Santos, JR, AG Exposito, JL Martinez Ramos, Distributed Contingency Analysis: Practical Issues, IEEE Transactions on Power Systems, Vol 14, No 4, Nov 1999, pp 1349-1354.

[65] Anderson, DM, BF Wollenberg, "Power-System Steady-State Security Analysis Using Vector Processing Computers", IEEE Transactions on Power Systems, v. 7(4), pp 1451-1455, Nov 1992.

[66] Alves AB, A Monticelli, "Static security analysis using pipeline decomposition", IEE-Proc-C Generation, Transmission and Distribution, v. 145(2), pp 105-110, Mar 1998.

[67] Stott, B., O Alsac, FL Alvarado, Analytical and Computation Improvements in Performance-Index Ranking Algorithms for Networks, International Journal of Electrical Power and Energy Systems, Vol 7, pp 154-160, July 1985.

[68] EPRI, Transmission System Reliability Methods, EPRI EL-2526, Vol 1, July 1982.

[69] Tinney, WF, V Brandwajn, SM Chan, Sparse Matrix Methods, IEEE Transactions on Power Apparatus and Equipment, PAS-104, pp 295-301, Feb 1985.

[70] Vaahedi, E, et al, Voltage stability contingency screening and ranking, IEEE Transactions on Power Systems, vol 14(1), pp 256-265, 1999.

[71] Singh, SN, Improved Contingency Selection Algorithm for Voltage Security Analysis, Electric Machines and Power Systems, Vol 26, No 8, 1998, pp 855-871.

[72] Mazumdar, M and DP Gaver, A Comparison of Algorithms for Computing Power Generating System Reliability Indices, IEEE Transactions on Power Apparatus and Systems, Vol PAS-103, No 1, Jan 1984, pp 92-99.

[73] Billonton, Roy, M Fotuhi-Firuzabad, S. Aboreshaid, Power System Health Analysis, Reliability Engineering and System Safety, Vol 55, 1997, pp 1-8.

[74] Mijuskovic, NA and D Stojnic, Probabilistic Real-Time Contingency Ranking Method, Electrical power and Energy Systems, Vol 22, 2000, pp 531-535.

[75] Billinton, R, PRS Kuruganty, A probabilistic assessment of transient stability in a practical multi-machine system, IEEE Transactions on Power Apparatus and Equipment, PAS-100, pp 3634-3642, 1981.

[75] Nahman, J and I Skokljev, Probabilistic Steady-State Power System Security Indices, Electrical Power and Energy Systems, Vol 21, pp 515-522, 1999.

[76] Jasmon, GB and LHCC Lee, New Contingency Ranking Technique Incorporating a Voltage Stability Criterion, IEE Proceedings-C, Vol 140, No 2, March 1993, pp 87-90.

[77] Benahmed, M, et al., A New Voltage Contingency Selection Method Using Corrected Solution Defined in Convergence Sense for Large Power Systems, 28th Universities Power Engineering Conference, 1993, Vol 2, pp 672-675.

[78] Leite da Sliva, AM, J Endrenyi, L Wang, Integrated Treatment of Adequacy and Security in Bulk Power System Reliability Evaluation, IEEE Transactions on Power Systems.

[79] C Fu and A Bose, Contingency Ranking Based on Severity Indices in Dynamic Security Analysis, IEEE Transactions on Power Systems, Vol 14, No 3, August 1999, pp 980-986.

[80] Chiang, H-D, C-S Wang, A Flueck, Look-ahead Voltage and Load Margin Contingency Selection Functions for Large-Scale Power Systems, IEEE Transactions on Power Systems, Vol, 12, No 1, Feb 1997, 173-180.

[81] Flatabo, N, et al, A method for calculation of margins to voltage instabilities applied on the Norwegian system for maintaining required security level, IEEE Transactions on Power Systems, v 8(2), pp 920-928, May 1993.

[82] Ejebe, GC, et al, Methods for contingency screening and ranking for voltage stability analysis of power systems, IEEE Transactions on Power Systems, v 11(1), pp 350-356, Feb 1996.

[83] Van Horne, PR, An Improved Method of Identifying and Ranking Critical Transmission Contingencies, paper presented at COPS Conference, Oklahoma City, March 1980.

[84] Chang, Chung-Liang and Yuan-Yih Hsu, A New Approach to Dynamic Contingency Selection, IEEE Transactions on Power Systems, Vol 5, No 4., pp 1524-1528, Nov 1990.

[85] Marceau, Richard, FD Galiana, Fourier Methods for Estimating Power System Stability Limits, IEEE Transactions on Power Systems, Vol 9, No 2, May 1994, pp 764-771.

[86] McCalley J, A Fouad, et al., A Risk-Based Security Index for Determining Operating Limits In Stability-Mediated Electric Power Systems, IEEE Transactions on Power Systems, Vol 12, No 3, August 1997, pp 1210-1219.

[87] Irizarry-Riviera, AA, JD McCalley, V Vittal, Computing Probability of Instability for Stability-Constrained Electric Power Systems, Electric Power Systems Research, Vol 42, 1997, pp 135-143.

[88] Dadu, JC, A Merlin, New probabilistic approach taking into account reliability and operation security in EHV power system planning at EDF, IEEE Transactions on Power Systems, V 1(3), pp 175-181, 1986.

[89] Nahman, J, B Babic, Probabilistic steady-state security analysis including substation generated outages, Electric Power Systems Research, Vol 35(1), pp 31-37, 1995.

[90] Castro, CA, A Bose, "Correctability of Voltage Violations in Online Contingency Analysis", IEEE Transactions on Power Systems, v. 9(3), pp1651-1657, Aug 1994.

[91] Castro CA, et al., "Correctability in Online Contingency Analysis", IEEE Transactions on Power Systems, v 8(3), pp 807-814, Aug 1993.

[92] Tinguely, C., et al., Knowledge base for An Expert System Used For Steady State Security Analysis, International Journal of Electrical Power and Energy Systems, Vol 16, No 1, 1994, pp 49-59.

[93] Christie, RD, SN Talukdar and JC Nixon, CQR: A Hybrid Expert System for Security Analysis, IEEE Transactions on Power Systems, Vol 5, No 4, Nov 1990, pp 1503-1509.

[94] Jadid S. and MR Rokni, An Expert System To Improve Power System Contingency Analysis, Electric Power Systems Research, Vol 40, 1997, pp 37-43.

[95] Chen RH, J Gao, et al., Multi-Contingency Preprocessing For Security Assessment using Physical Concepts and CQR with Classification, IEEE Transactions on Power Systems, Vol 8, No 3, Aug 1993, pp 840-848.

[96] Van Cutsem, T. et al, Decision Tree Approaches to Voltage Security Assessment, IEE Proceedings-C, Vol 140, No 3, May 1993, pp 189-198.

[97] Zhu, JZ, G Xu and MR Irving, Automatic Contingency Selection and Ranking Using an Analytical Hierarchical Process, Electric Machines and Power Systems, Vol 26, 1998, pp189-198.

[98] Neibur, D, Des Reseaux De Neurones Artificiels Appliques Aux Reseaux Electriques, Electra, No 159, Avril 1995, pp76-101.

[99] Sidhu, TS and L Cui, Contingency Screening for Steady-State Security Analysis By Using FFT and Artificial Neural Networks, IEEE Transactions on Power Systems, Vol 15, No 1, Feb 2000, pp 421-426.

[100] Srivastava, L., SN Singh and J Sharma, A Hybrid Neural Network Model for Fast Voltage Contingency Screening and Ranking, Electrical Power and Energy Systems, Vol 22, 2000, pp 35-42.

[101] Wan HB and AO Ekwue, Artificial Neural Network Based Contingency Ranking Method For Voltage Collapse, Electrical Power and Energy Systems, Vol 22, 2000, pp 349-354.

[102] Lo KL, LJ Peng, et al., Fast Real Power Contingency Ranking Using a Counterpropagating Network, IEEE Transactions on Power Systems, Vol 13, No 4, Nov 1998, pp 1259-1264.

[103] Riquelme, J., A Gomez, JL Martinez, " Topology-independent artificial neural network for overload screening", Neurocomputing 23 (1998), pp 151-160.

[104] Niebur, D., et al., Artificial neural networks for power systems: a literature survey, Engineering Intelligent Systems, Vol 1(3), 1993.

[105] Schaefer, KF, JF Verstege, Adaptive selection algorithm for masking effect compensation in contingency selection algorithm, IEEE Transactions on Power Systems, Vol 5(2), pp 539-546, 1990.

[106] Mahadev, PM, RD Christie, Envisioning Power System Data: Vulnerability and Severity Representations for Static Security Assessment, IEEE Transactions on Power Systems, Vol 9, No 4, Nov 1994, pp 1915-1920.

[107] Cote JW, CC Liu, Voltage Security Assessment Using Generalized Operational Knowledge, IEEE Transactions on Power Systems, Vol 8, No 1, Feb 1993, pp 28-34.

[108] Litynski DM, M Grabowski M, WA Wallace, The relationship between three-dimensional imaging and group decision making: An exploratory study, IEEE Transactions on Systems, Man and Cybernetics, Part A – Systems and Humans, Vol 27(4), pp 402-411, July 1997.

[109] Billinton, Roy and Sudhir Kumar, Adequacy Evaluation of a Composite Power System – A Comparative Study of Existing Computer Programs, Canadian Electrical Association, Spring Meeting, March 1985, Montreal.

[110] Beshir, MJ, TC Cheng and ASA Farag, Comparison of Monte Carlo Simulation and State Enumeration Based Adequacy Assessment Programs: CREAM and COMREL, IEEE (?)

[111] National Communications System, Management of Stressed Switched Networks: Level I Report Extension, , NCS TIB 92-13, September 1992.

[112] National Communications System, Management of Stressed Facility Networks: Level II Report Extension, NCS TIB 92-14, September 1992.

[113] S. Milgram, "The Small World Problem," *Psychology Today*, vol. 2, pp. 60-67, 1967.

[114] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," Nature, vol. 393, pp. 440-442, 1998.

[115] D. Watts, Small Worlds: The Dynamics of Networks Between Order and Randomness, Princeton University Press, Princeton, NJ 1999].

[116] Albert, R. Jeong, H. Barabasi, A.-L, Diameter of the World Wide Web, Nature 401, 130-131, 1999.

[117] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Breakdown of the Internet under intentional attack," Physical Review Letters, vol. 86, pp. 3682-3685, 2001.

[118] Cormen, T, Leiserson, C., Rivest, R. Stein, C., Introduction of Algorithms, 2nd ed., MIT Press, Cambridge, MA, 2001.

[119] Albert, R. Jeong, H. Barabasi, A.-L, Error and Attack Tolerance of Complex Networks, Nature 406, 378-382, July 2000.

[120] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Resilience of the Internet to random breakdowns," Physical Review Letters, vol. 85, pp. 4626-4628, 2000.

[121] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Comment on "Breakdown of the Internet under intentional attack" : Reply : art. no. 219802," Physical Review Letters, vol. 8721, pp. 9802-9802, 2001.

[122] Atkin, R. H., Combinatorial Connectivities in Social Systems, Birkhauser Verlag. Basel und Stuttgart, 1977.

[123] Cabral, L. M., Task analysis. A polyhedral dynamics approach *Proceedings of the Human Factors Society*, vol. pp. 1295-1298, 1990.

[124] J.L. Casti. *Connectivity, Complexity, and Catastrophe in Large-Scale Systems*, John Wiley & Sons, 1979.

[125] Duckstein, L., Bartels, P. H., and Weber, J. E., Organization of a knowledge base by Q-analysis. *Applied Mathematics and Computation*, vol. 26, no. 4, pp. 289-301, Jun, 1988.

[126] Duckstein, L., Kempf, J., and Casti, J., Design and Management of Water-Resources System by Polyhedral Dynamics *Hydrological Sciences Journal-Journal Des Sciences Hydrologiques*, vol. 27, pp. 193-194, 1982.

[127] Robinson, D. and Duckstein, L., Polyhedral Dynamics as a Tool for Machine-Part Group Formation. *International Journal of Production Research*, vol. 24, no. 5, pp. 1255-1266, Sep, 1986-Oct 31, 1986.

[128] Eberhart and Yuhui, S., "Particle swarm optimization: developments, applications and resources," *IEEE International Conference on Evolutionary Computation,* Seoul, South Korea; May 27, 2001, pp. 81-86.

[129] Eberhart, R. and Kennedy, J., "A new optimizer using particle swarm theory," *International Symposium on Micromechatronics and Human Science,* Nagoya, Japan, pp. 39-43.

[130] Eberhart, R. C. and Shi, Y., "Comparing inertia weights and constriction factors in particle swarm optimization," *IEEE International Conference on Evolutionary Computation,* La Jolla, CA, USA, pp. 84-88.

[131] Eberhart, R. C. and Xiaohui, H., "Human tremor analysis using particle swarm optimization," *The 1998 IEEE International Conference on Evolutionary Computation Proceedings,* Washington, DC, USA, pp. 0-1930.

[132] Eberhart, R. C. and Yuhui, S., "Tracking and optimizing dynamic systems with particle swarms," *IEEE International Conference on Evolutionary Computation,* Seoul, South Korea, pp. 94-100.

[133] Floyd, C. E., Yuhui, S., and Eberhart, R. C., "Empirical study of particle swarm optimization," *IEEE International Conference on Evolutionary Computation,* pp. 1945-1950.

[134] Fukuyama, Y. and Yoshida, H., "A particle swarm optimization for reactive power and voltage control in electric power systems," *IEEE International Conference on Evolutionary Computation,* Seoul, South Korea, pp. 87-93.

[135] He, Z., Wei, C., Yang, L., Gao, X., Yao, S., Eberhart, R. C., and Yuhui, S., "Extracting rules from fuzzy neural network by particle swarm optimisation," *IEEE International Conference on Evolutionary Computation,* Anchorage, AK, USA, pp. 74-77.

[136] Jinchun, P., Yaobin, C., and Eberhart, R., Battery pack state of charge estimator design using computational intelligence approaches IEEE-0275.

[137] Kennedy, J. and Eberhart, R., "Particle swarm optimization," *IEEE International Conference on Neural Networks,* Perth, WA, Australia, pp. 1942-1948.

[138] Kennedy, J. and Eberhart, R. C., "A discrete binary version of the particle swarm algorithm," *IEEE International Conference on Systems, Man, and Cybernetics,* Orlando, FL, USA, pp. 4104-4108, October 12, 1997.

[140] Kennedy, J. and Eberhart, R. C. *Swarm Intelligence*, San Francisco, CA: Academic Press, 2001.

[141] Schoenauer, M., Eberhart, R. C., and Xiaohui, H., "Human tremor analysis using particle swarm optimization," *IEEE International Conference on Evolutionary Computation,* pp. 1927-1930.

[142] Shi, Y. and Eberhart, R., "A modified particle swarm optimizer," *IEEE International Conference on Evolutionary Computation,* Anchorage, AK, USA, pp. 69-73.

[143] Shi, Y. and Eberhart, R. C., "Empirical study of particle swarm optimization," *The 1998 IEEE International Conference on Evolutionary Computation Proceedings,* pp. 0-1950.

[144] Yoshida, H., Fukuyama, Y., Takayama, S., and Nakanishi, Y., "A particle swarm optimization for reactive power and voltage control in electric power systems considering voltage security assessment," *IEEE International Conference on Systems, Man, and Cybernetics,* Tokyo, Japan, pp. 497-502.

[145] Yoshida, H., Kawata, K., Fukuyama, Y., Takayama, S., and Nakanishi, Y., A particle swarm optimization for reactive power and voltage control considering

voltage security assessment *IEEE Transactions on Power Systems* , vol. 15, pp. 1232-1239, Nov, 2000.

[146] Yuhui, S. and Eberhart, R. C., "Fuzzy adaptive particle swarm optimization," *IEEE International Conference on Evolutionary Computation,* Seoul, South Korea, pp. 101-106.

Appendix A. Momentum versus Velocity Summaries

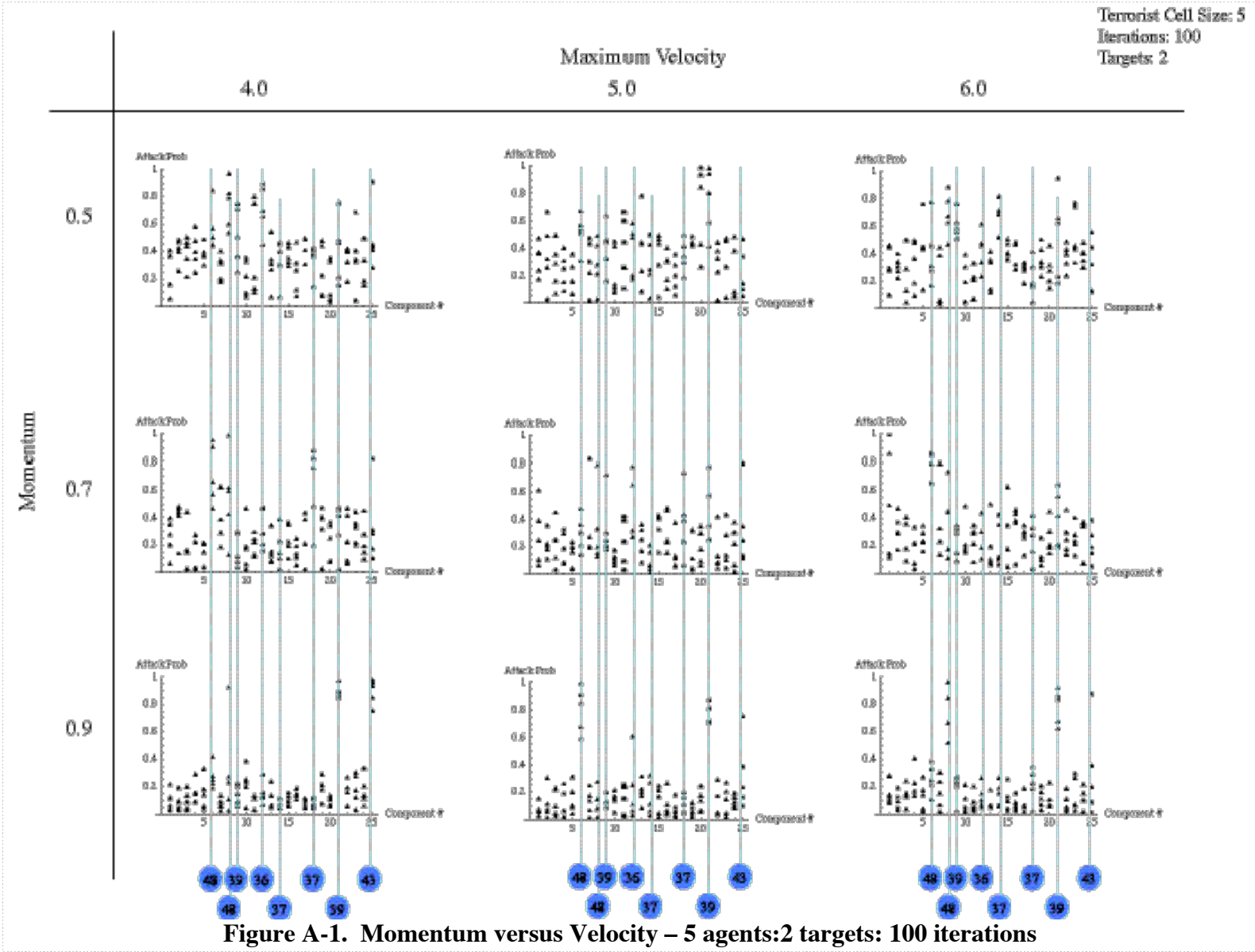


Figure A-1. Momentum versus Velocity – 5 agents:2 targets: 100 iterations

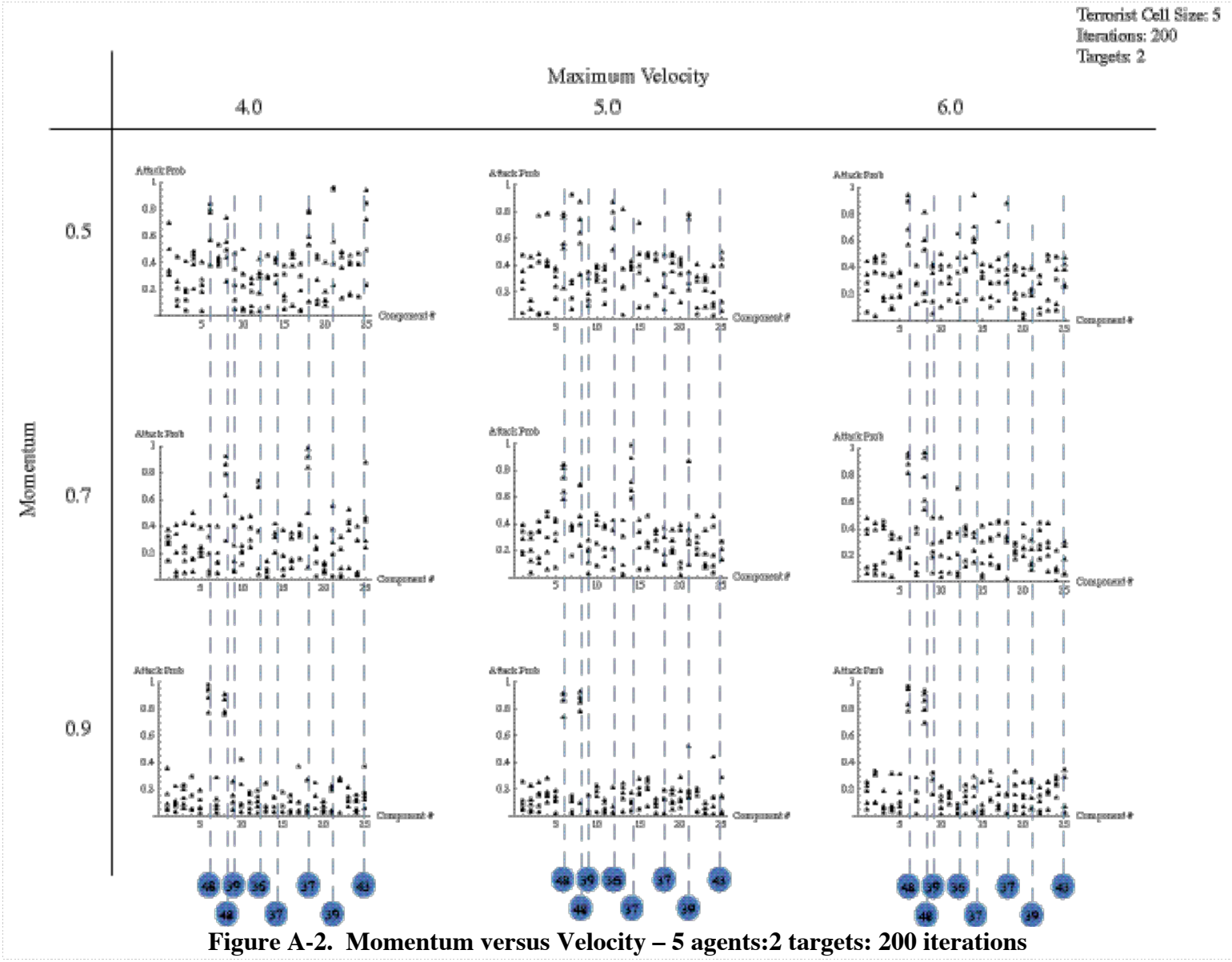


Figure A-2. Momentum versus Velocity – 5 agents:2 targets: 200 iterations

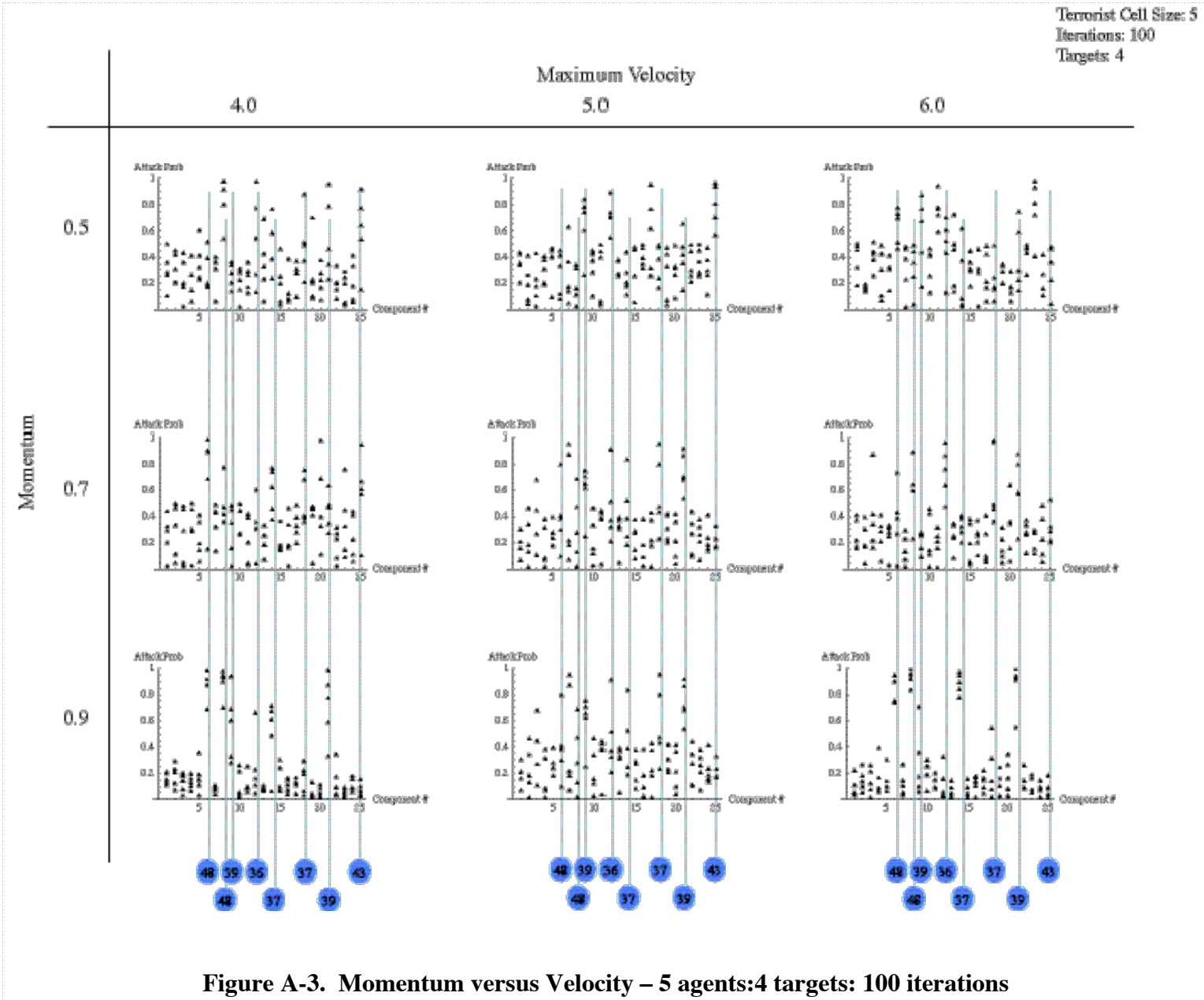


Figure A-3. Momentum versus Velocity – 5 agents:4 targets: 100 iterations

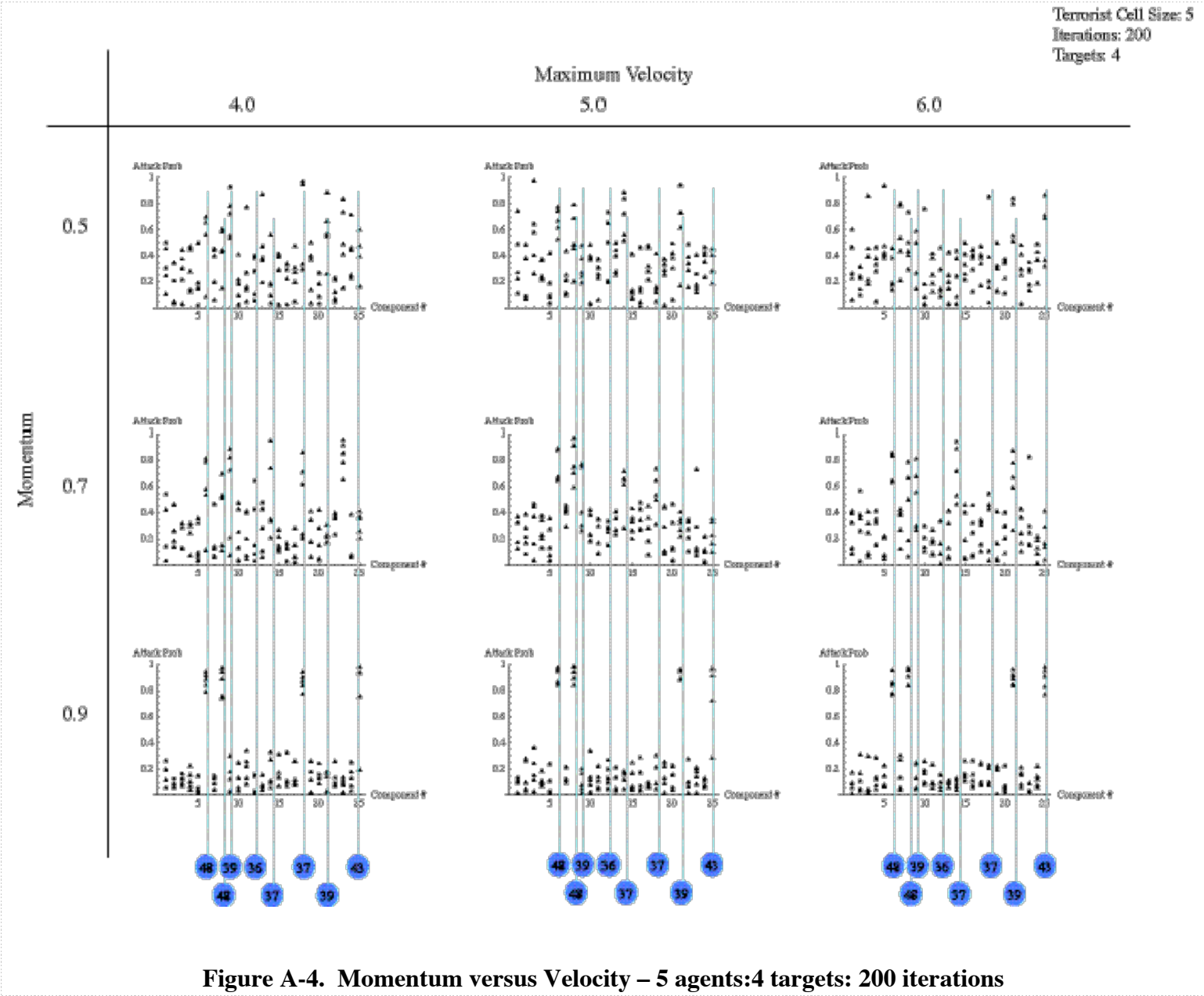


Figure A-4. Momentum versus Velocity – 5 agents:4 targets: 200 iterations

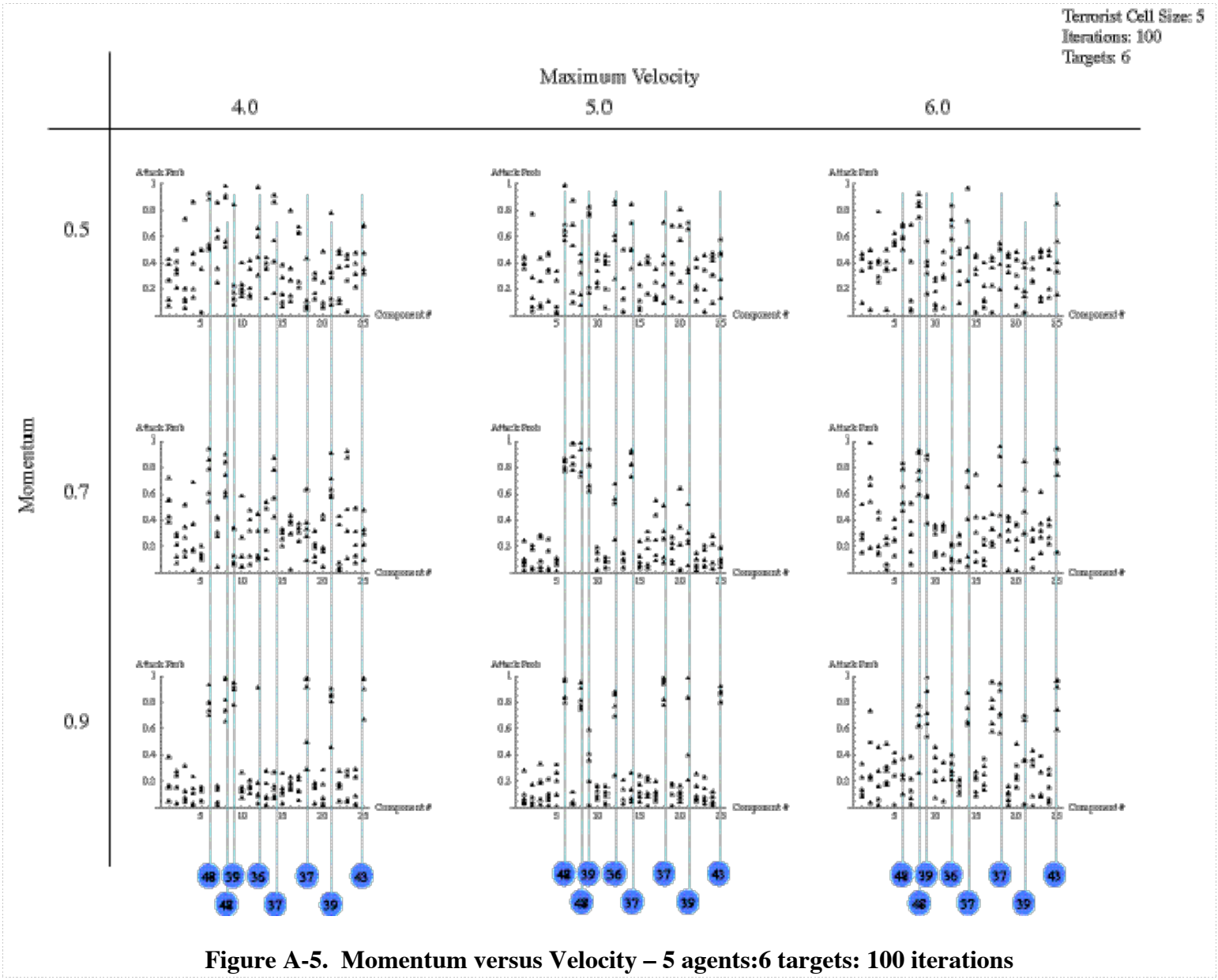


Figure A-5. Momentum versus Velocity – 5 agents:6 targets: 100 iterations

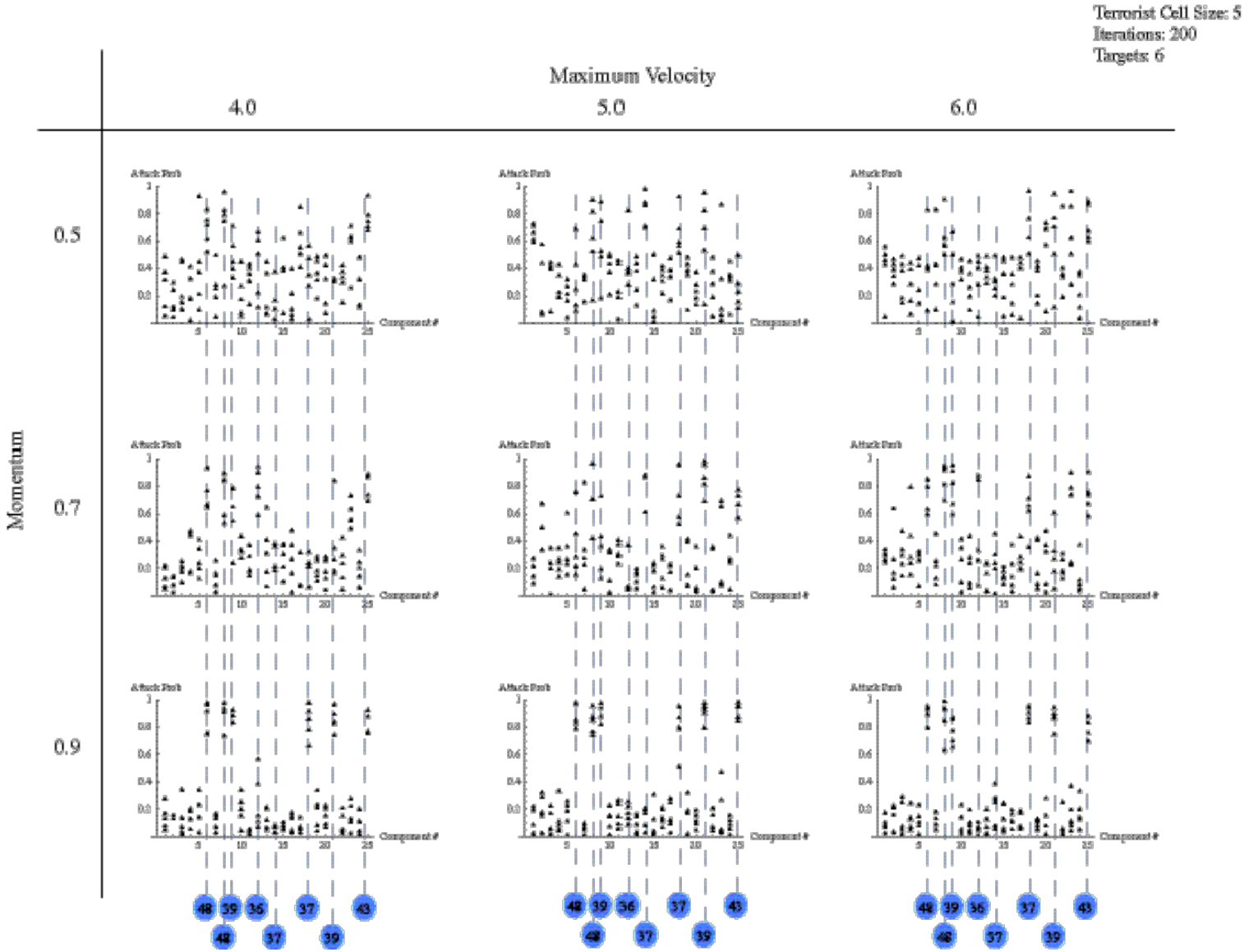
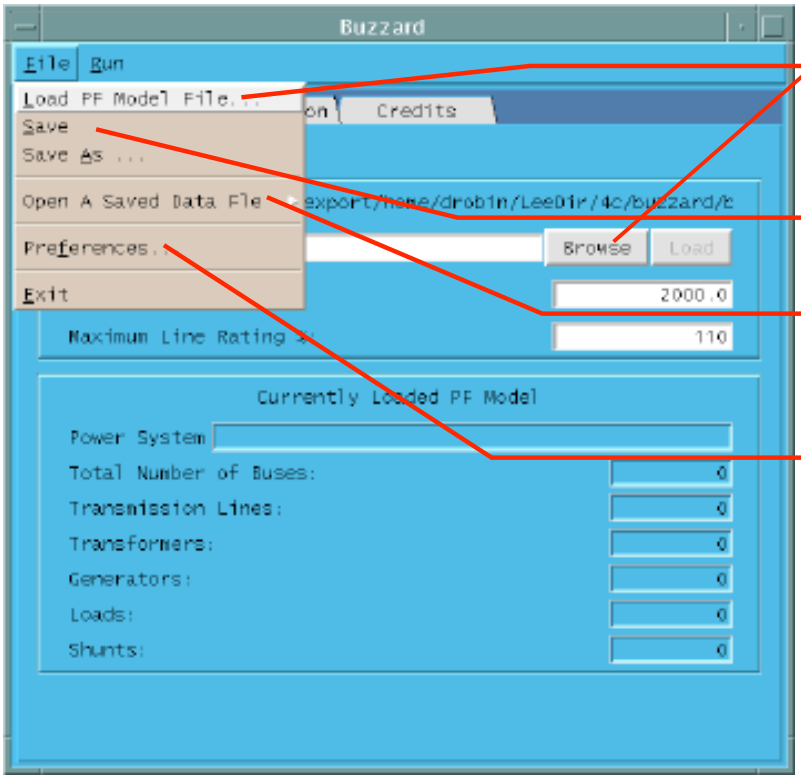


Figure A-6. Momentum versus Velocity – 5 agents:6 targets: 200 iterations

Appendix B. Buzzard User Interface

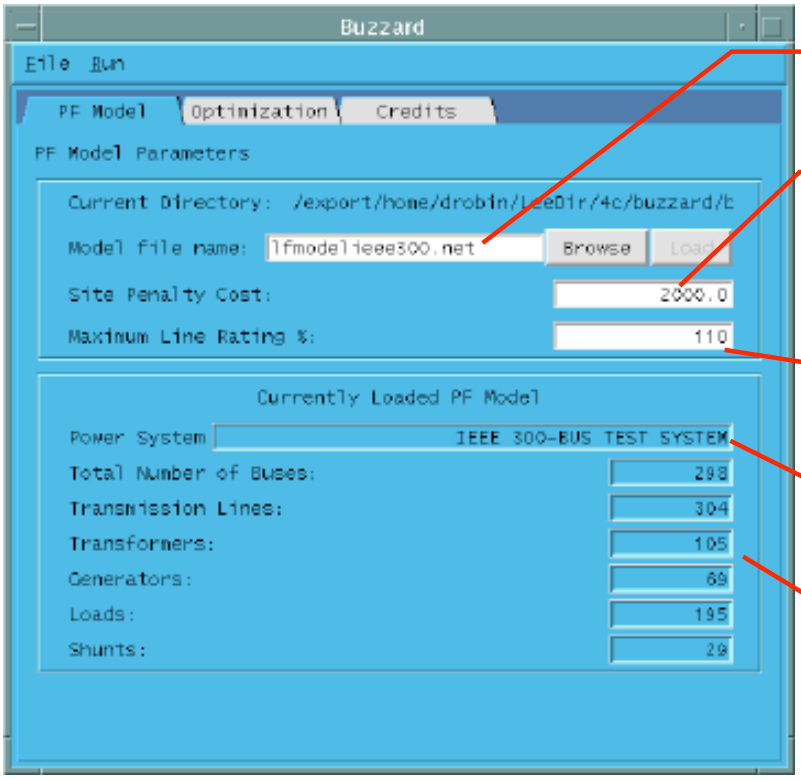


Load a GE formatted power flow file

After making changes the user can save

Load an output data file from a previoius analysis

Change interface preferences



File name of data

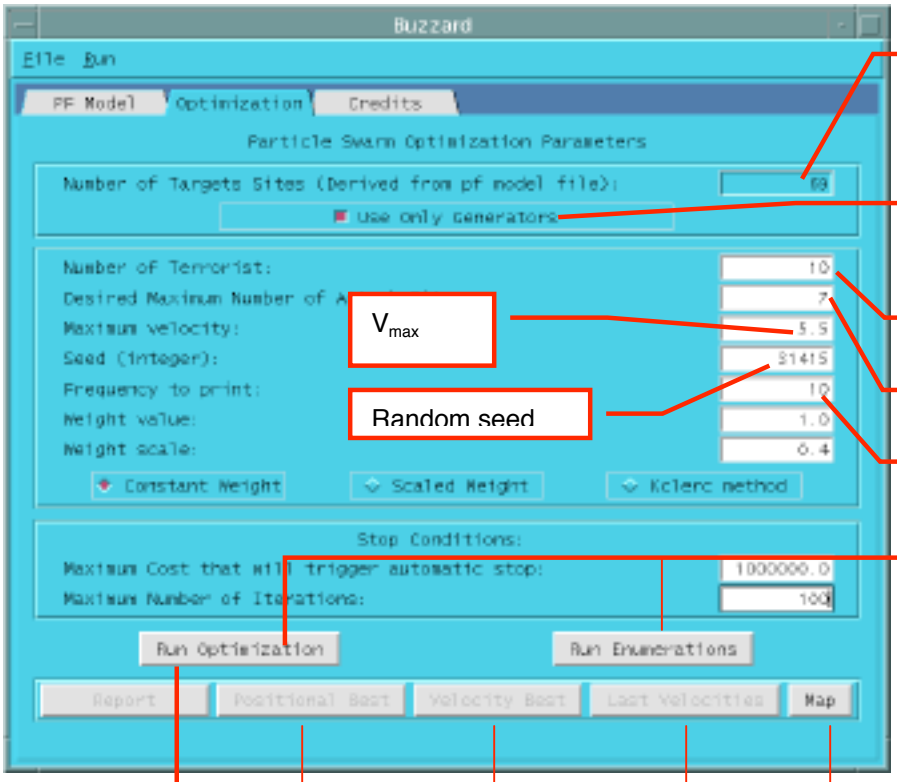
Cost penalty for each target in excess of number of allowable targets

Line overrating failure criteria

Model name from GE file

Node specific information pulled directly from data file

Appendix B. Buzzard User Interface



Number of possible targets – culled from input data file

Option to only allow generators to be disrupted

V_{max}

Random seed

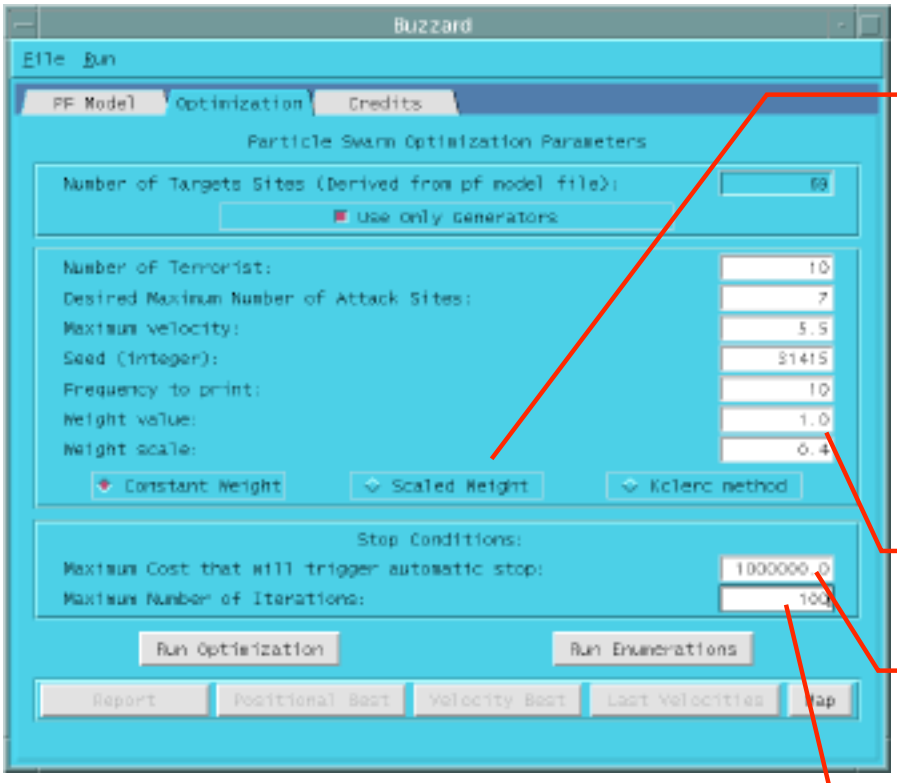
Number of terrorists in each 'cell'

Number of allowable attack sites

Frequency to print to report file

Run in optimization mode or enumeration mode to find optimal target set

Each output option opens a new window: text report, positional best, velocity best, last velocities or a map of network. Sample windows presented below

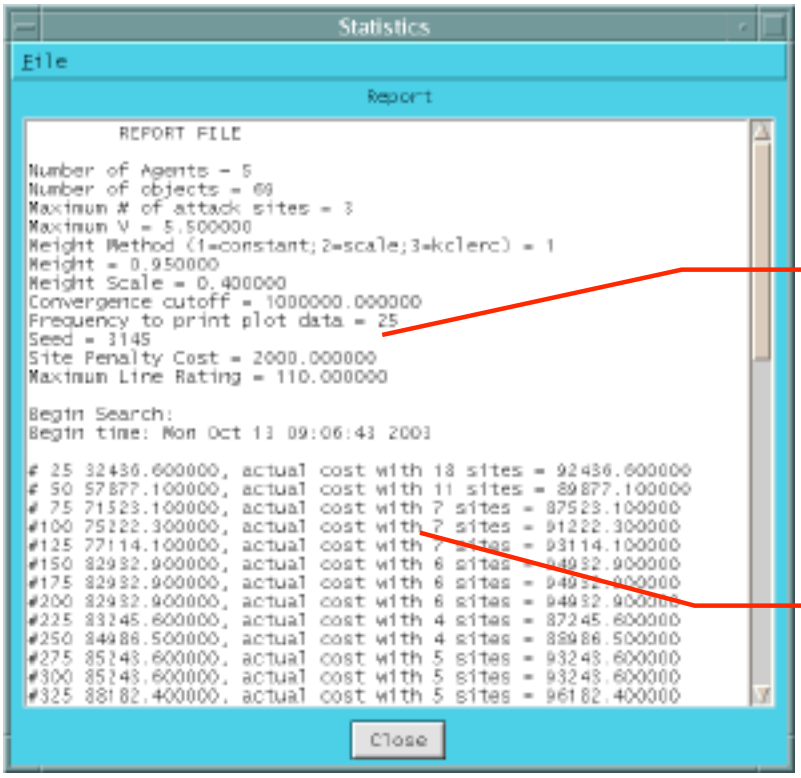


Type of weighting function to apply to velocity to assist in convergence. A 'constant weight' applies an equal factor specified by the (Weight Value) to each successive velocity estimate while a scaled weight changes the based on the number of targets over the maximum allowed. The Clerc method is an adaptive weighting method common in non-integer swarm applications.

Parameters of the different weighting functions

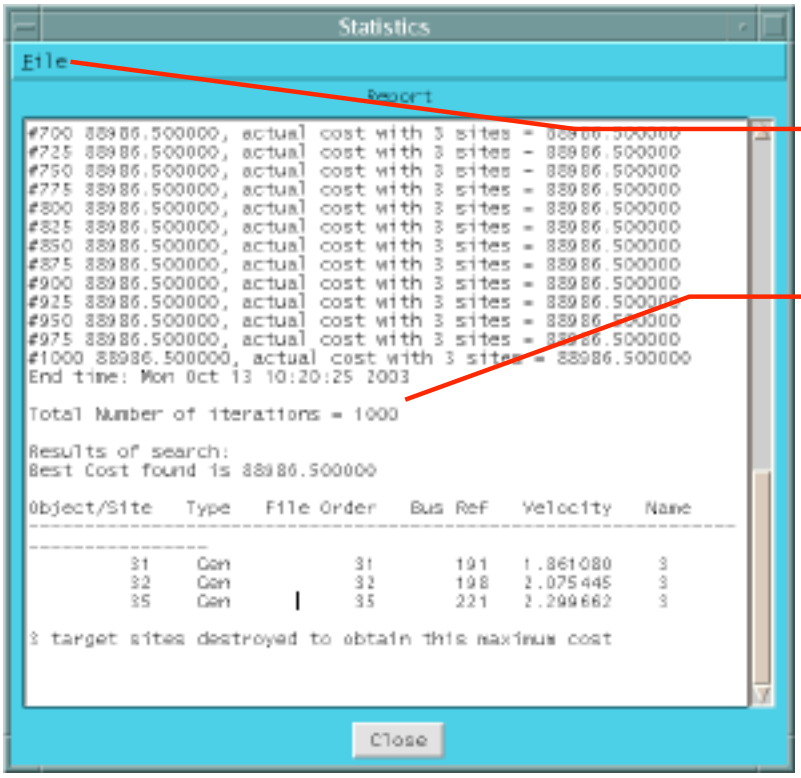
Maximum cost value to prevent runaway of optimization algorithm

Maximum number of iterations permitted



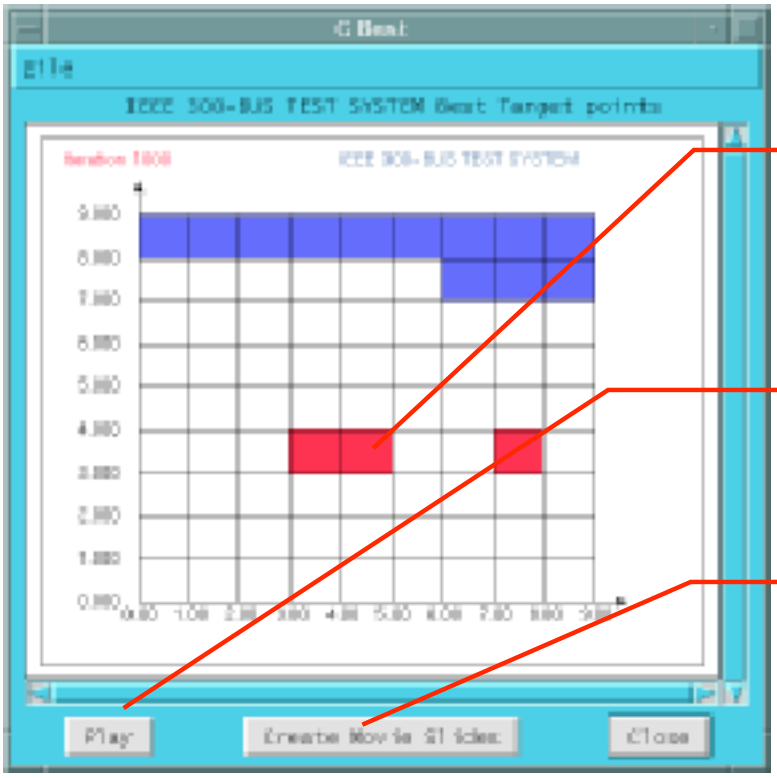
Top of report file provides summary of all input data.

Real cost, penalty function cost and number of target sites are presented for each iteration. Iteration increment is user input.



Report can be saved for later printing or review

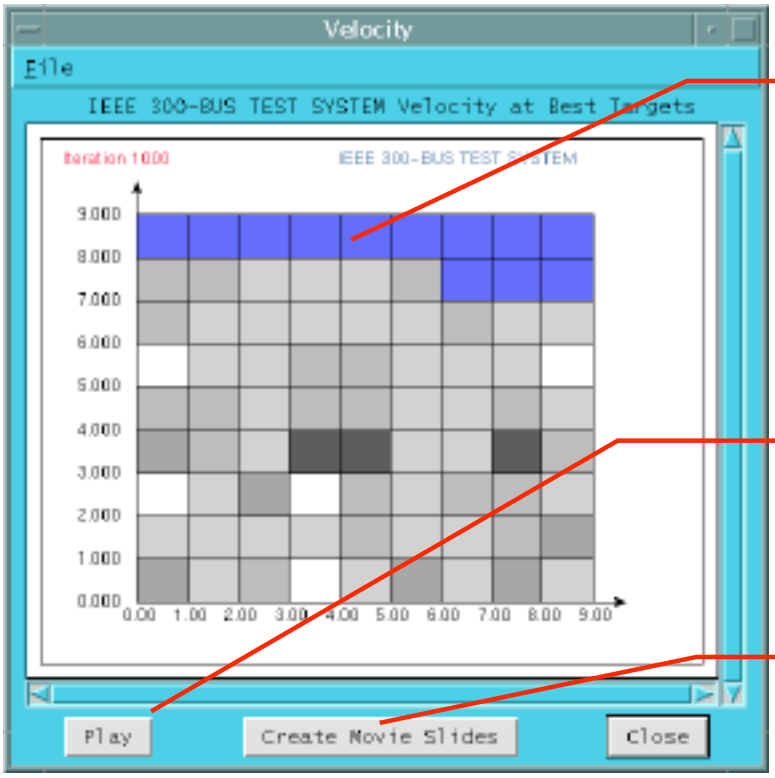
Summary of results is provided at end of report file. Target name, buss reference number and velocity associated with each target are provided.



A NxN square is depicted where each square corresponds to a particular target. Squares that are shaded BLUE are not used. RED squares are associated with nodes that finally selected as targets.

The PLAY button run through the simulation and displays the nodes as they are selected/rejected as targets

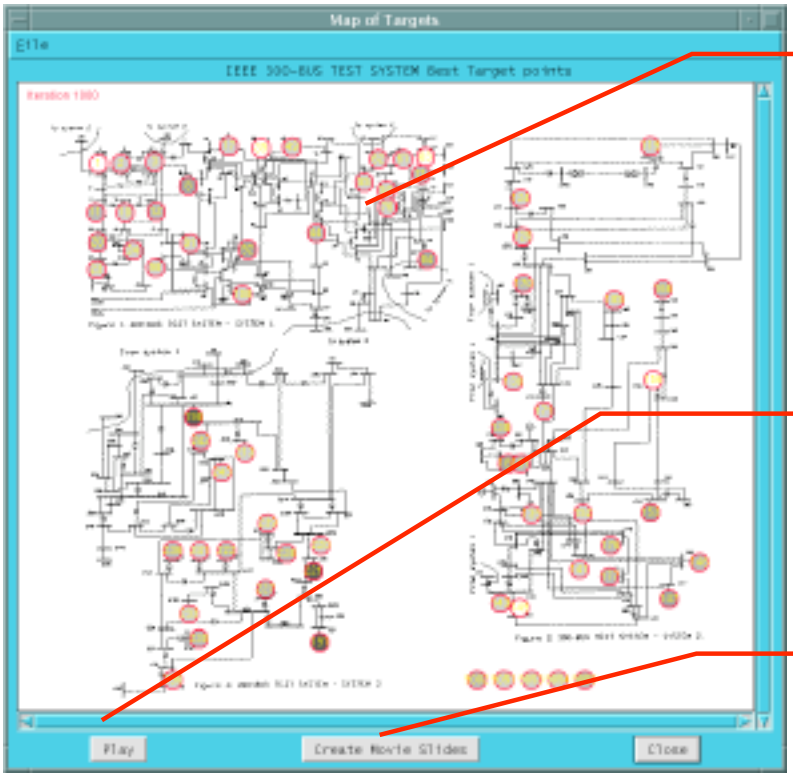
The CREATE MOVIE SLIDES button generates a series of postscript files that can be input to a Quicktime movie.



Similar to the best target window, a NxN square is depicted where each square corresponds to the velocity of a particular target during the simulation. Squares that are shaded BLUE are not used. Shading ranges from white to black. The darker the shading the higher the velocity for that target and the higher the likelihood for selection as a target in the simulation.

The PLAY button run through the simulation and displays the nodes as they are selected/rejected as targets

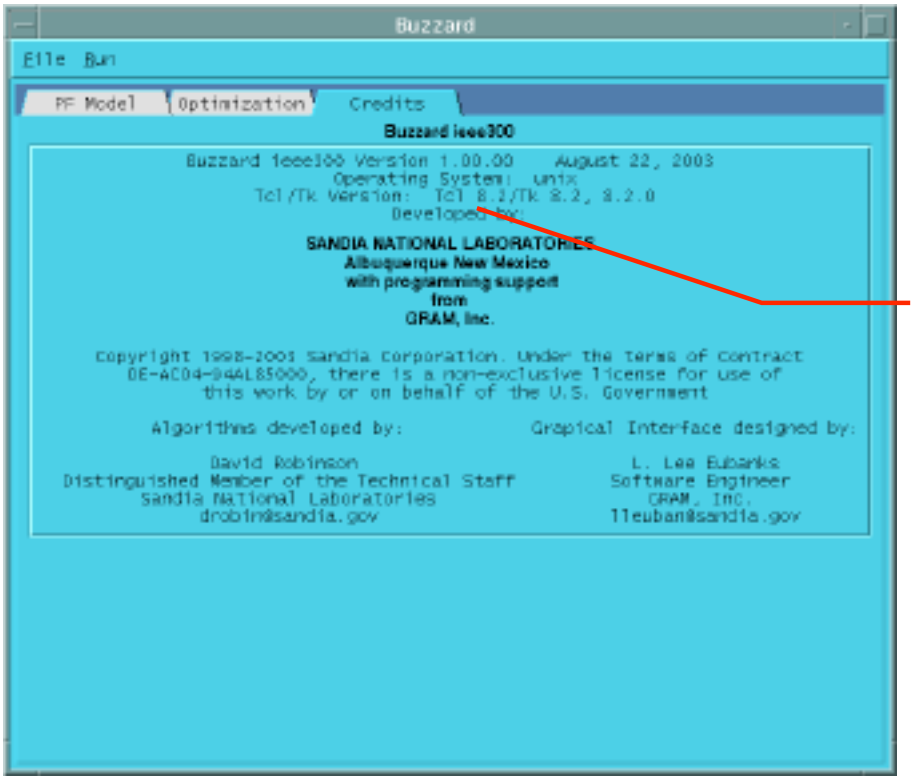
The CREATE MOVIE SLIDES button generates a series of postscript files that can be input to a Quicktime movie.



Velocities overlayed on power grid. Shading ranges from white to black. The darker the shading the higher the velocity for that target and the higher the likelihood for selection as a target in the simulation

The PLAY button run through the simulation and displays the nodes as they are selected/rejected as targets

The CREATE MOVIE SLIDES button generates a series of postscript files that can be input to a Quicktime movie.



Who did what with what…

Distribution

50	MS 0748	D. G. Robinson, 6861
1	MS 0748	R. G. Cox, 6861
1	MS 9018	Central Technical Files, 8945-1
2	MS 0899	Technical Library, 9616